96920-4783

OCTOBER 1900

ANNALS OF MATHEMATICS

(FOUNDED BY ORMOND STONE)

EDITED BY

ORMOND STONE W. E. BYERLY H. S. WHITE

W. F. OSGOOD F. S. WOODS

PUBLISHED UNDER THE AUSPICES OF HARVARD UNIVERSITY

SECOND SERIES Vol. 2 NO. 1

FOR SALE BY

THE PUBLICATION OFFICE OF HARVARD UNIVERSITY

2 University Hall, Cambridge, Mass., U. S. A.

London: LONGMANS, GREEN & CO.
39 Paternoster Row

Leipsig: OTTO HARRASSOWITZ
Querstrasse 14

JUL 18 1901

1900 – 1901

ANNALS OF MATHEMATICS

(FOUNDED BY ORMOND STONE)

EDITED BY

ORMOND STONE W. E. BYERLY H. S. WHITE
W. F. OSGOOD F. S. WOODS

PUBLISHED UNDER THE AUSPICES OF HARVARD UNIVERSITY

SECOND SERIES Vol. 2

FOR SALE BY
THE PUBLICATION OFFICE OF HARVARD UNIVERSITY
2 University Hall, Cambridge, Mass., U. S. A.

LIBRARY
LELAND STANFORD JUNIOR
UNIVERSITY

London: LONGMANS, GREEN & Co.
39 Paternoster Row

Leipzig: OTTO HARRASSOWITZ
Querstrasse 14

WIENER'S THEORY OF DISPLACEMENTS, WITH AN APPLICATION TO THE PROOF OF FOUR THEOREMS OF CHASLES.*

By Arthur Sullivan Gale.

The foundations of the theory of finite displacements in space were laid by Chasles in a series of papers published in 1860–61. Of particular interest and importance are the theorems† relating to the displacement of a right line and plane figure which form the basis of an important paper by Study.‡ From these theorems Study derives a variety of others including the resolution of any displacement into the product of two involutory displacements given by Wiener.§ It is the object of this paper to give some account of Wiener's work in the theory of displacements, and to apply his methods to the proof of the four theorems of Chasles forming the basis of Study's paper. Study remarks‖ that this application can be readily made.

1. Wiener's Theory of Displacements. In Wiener's work the fundamental displacement is a *reflection in a line* (*Umwendung*), which consists of a rotation through π or an orthogonal reflection in the axis of the rotation. A reflection in a line l is denoted by the symbol (l). The most important property of a reflection in a line is that it is *involutory*, that is, if performed twice it gives the identical transformation. Other important involutory transformations are a *reflection in a plane* and a *reflection in a point*: the first is such that the chord joining any pair of corresponding points is perpendicular at its middle point to a given plane: the second is such that the middle point of the chord joining any pair of corresponding points is a given point. These are both special cases of the general *symmetry transformation* (*Umlegung*) which transforms a given configuration into any second configuration whose parts are equal to those of the first but are arranged in the opposite order.

---

* This paper was read before the American Mathematical Society at the meeting of April 28, 1900.

† *Compt. Rend.*, Vol. 51, pp. 909, 940 (1860). Proofs of these theorems were first published by Brisse, *Jour. de Math.* Series 2, Vol. 19, pp. 253–258 (1874).

‡ *Math. Annalen*, Vol. 39, pp. 441–566 (1891).

§ *Leipziger Berichte*, Vol. 42, p. 76 (1890).

‖ *l. c.*, p. 469.

Let us consider with Wiener* the effect of combining reflections in the lines t_1 and t_2, the indices denoting the order in which the reflections are to take place. Three cases present themselves.

1°. Let t_1 and t_2 be *parallel*. If any point P be reflected in t_1 and then in t_2 its final position P' is evidently such that the line PP' is equal both in magnitude and in direction to twice the perpendicular distance from t_1 to t_2. The product $(t_1\, t_2)$ is then a *translation*.

2°. Let t_1 and t_2 *intersect*. The points in their common perpendicular at the point of intersection are unchanged by the displacement $(t_1\, t_2)$, which is therefore a *rotation*. By starting from a point on t_1 and reflecting it in t_2, it is seen that the angle of the rotation is twice the angle from t_1 to t_2. If t_1 is perpendicular to t_2 the product $(t_1\, t_2)$ is a *reflection in a line*.

3°. Let t_1 and t_2 be *skew lines*. Let L be their common perpendicular cutting t_1 at a and let t' be a line through a parallel to t_2. Then since a reflection in a line is involutory

$$(t_1\, t_2) = (t_1\, t'\, t'\, t_2) = (t_1\, t')\ (t'\, t_2)$$

$(t_1 t')$ is a rotation about L and $(t' t_2)$ is a translation parallel to L. Hence the product $(t_1\, t_2)$ is a *screw displacement* (*Schraubung*). If t_1 is perpendicular to t_2 the product is a *semi-screw displacement* (*Umschraubung*) *i. e.*, a rotation through π about a line combined with a translation parallel to that line.

Conversely we at once deduce the following resolutions.

Every translation may be effected in ∞^3 *ways by combining reflections in two lines;* these lines are parallel, the vector distance from the first to the second being equal to half the vector of the translation.

Every rotation may be effected in ∞^2 *ways by combining reflections in two lines;* the lines are perpendicular at the same point to the axis of the rotation, the angle between them being equal to half the angle of the rotation. For a *reflection in a line* the angle is $\pi/2$.

Every screw displacement may be effected in ∞^2 *ways by combining reflections in two lines;* the lines are perpendicular to the axis of the displacement, the distance and angle between them being equal respectively to half the altitude (*Schraubungshöhe*) and turn (*Schraubungswinkel*) of the displacement. For a *semi-screw displacement* the angle is $\pi/2$.

In any displacement space is regarded as rigid and hence a displacement

* *Leipziger Berichte*, Vol. 42, pp. 16–20.

is determined by the initial and final positions of any triangle. This affords a simple proof of Wiener's fundamental theorem:

*Every displacement in space may be effected by combining two reflections in lines.**

Consider two congruent triangles in any relative positions. If they be so situated in a plane that they may be brought into coincidence by a displacement in the plane then they may be brought into coincidence either by a rotation (or a reflection in a line) about a line perpendicular to their plane or by a translation parallel to it. In these cases the theorem follows at once from the resolutions given above.

Whatever be the positions of the two triangles they may be readily brought into the positions just considered. When the planes of the triangles intersect this may be accomplished by rotating one about the line of intersection; when the planes of the triangles are parallel or coincident it may be accomplished either by a translation perpendicular to the planes, or by a reflection in a line parallel to the planes and half way between them.† A displacement in a plane will now bring the two triangles into coincidence. It only remains to show that the product of two rotations, either or both of which may degenerate into a reflection in a line or into a translation, is always equivalent to the product of two reflections in lines. Let (R_1) and $(\ _2)$ be the two rotations and let t' be the common perpendicular to the axes R_1 and R_2. We may choose the lines t_1 and t_2 so that

$$(R_1) = (t_1 t') \qquad \text{and} \qquad (R_2) = (t' t_2)$$

and hence

$$(R_1 R_2) = (t_1 t' t' t_2) = (t_1 t_2).$$

The product of the two rotations is thus replaced by the product of two reflections in lines. The reasoning requires no modification if one or both of the rotations degenerate into reflections in lines. If (R_1) be a translation we may take for t' any line meeting R_2 and perpendicular to it, and in a plane perpendicular to the direction of the translation (R_1). If both (R_1) and (R_2) be translations we may take for t' any line perpendicular to the directions of (R_1) and (R_2).

An immediate result of this theorem is that the most general displacement is a screw displacement, for this is the most general effect of combining two

* *l. c.* p. 76. The proof given here is due to Professor P. F. Smith.

†This covers the case of symmetrical triangles in a plane.

reflections in lines. If this well-known result be presupposed Wiener's fundamental theorem requires no proof other than the resolution which precedes it; the beauty of Wiener's work, however, is that it serves so admirably as an introduction to the subject. We indicate in passing two other important elementary results of the theory as thus far developed. The method just employed in considering the product of two rotations lends itself with equal readiness to the construction of the displacement which is the product of two screw displacements.* The displacements involved in the preceding proof can be readily constructed and replaced by two reflections in lines when the relative positions of the triangles are given; by combining the two reflections in lines we obtain the displacement which transforms a given triangle into a given congruent triangle.†

2. An Application of Wiener's Methods. By means of Wiener's fundamental theorem we shall in different ways resolve any displacement into the product of two transformations such that all the points of an arbitrarily chosen line or plane shall be invariant with respect to the first transformation. The theorems given by Chasles will follow immediately from the properties of the second transformation.

The following resolutions are such that the points of an arbitrary line are invariant with respect to the first displacement.

A straight line R being given, every displacement in space may be resolved into a rotation about R followed by a semi-screw displacement.‡

We may resolve any displacement (T) into the product $(t_1\, t_2)$ of reflections in lines so that the line t_1 shall be perpendicular to R. Let t' be a line perpendicular to R at its intersection with t_1 and also perpendicular to t_2. Then

$$(T) = (t_1\, t_2) = (t_1\, t'\, t'\, t_2) = (t_1\, t')\ (t'\, t_2),$$

$(t_1\, t')$ is a rotation about R and $(t'\, t_2)$ is a semi-screw displacement whose axis is the common perpendicular to t' and t_2.

A straight line R being given, every displacement in space may be resolved into a rotation about R followed by a second rotation (or by a translation).§

---

*Wiener, *l. c.* p. 21 and note p. 83. Halphen, *Nouv. Ann. de Math.*, Series 3, Vol. 1, p. 296 (1882). Burnside, *Messenger of Math.*, Vol. 19, p. 104 (1889).

†*Cf.* Wiener, *l. c.*, p. 77.

‡ This theorem is due to Study; *l. c.*, p. 465.

§ This theorm is due to Chasles; *Compt. Rend.* Vol. 52, p. 79 (1861).

Resolving (T) as above let now t' be perpendicular to R at its intersection with t_1 and let t' also intersect t_2 (if t_2 is perpendicular to R let t' be parallel to t_2.) Then

$$(T) = (t_1\, t_2) = (t_1\, t'\, t'\, t_2) = (t_1\, t')\ (t'\, t_2),$$

$(t_1\, t')$ is a rotation about R and $(t'\, t_2)$ is a rotation about the common perpendicular to t' and t_2 at their point of intersection (or a translation through twice the vector distance from t' to t_2).

In these resolutions the axis of the first displacement is arbitrary and hence *every displacement of a right line may be effected in either one of two ways:* 1° *by a semi-screw displacement;* 2° *by a rotation* (*or translation*). Two of the theorems of Chasles follow at once.

THEOREM I. *If a line be displaced the middle points of the chords joining congruent points lie on a line or are identical.*

These points will lie on the axis of the semi-screw displacement by which the displacement may be effected, and they will be identical if that axis is perpendicular to the given line.

THEOREM II. *If a line be displaced the planes perpendicular to the chords joining congruent points at their middle points pass through a line* (*or are parallel*) *or are identical.*

The planes in question will pass through the axis of the rotation by which the displacement may be effected. They will coincide if the axis of the rotation and the given line are co-planar. (If the displacement be a translation the planes will be parallel, or identical if the direction of the translation is perpendicular to the given line.)

To obtain the corresponding theorems relating to plane figures we seek to resolve a displacement into the product of two transformations such that the points of an arbitrary plane shall be invariant with respect to the first transformation. A simple transformation other than the identical transformation which will leave the points of an arbitrary plane invariant is a reflection in that plane. If we reflect any given configuration in any plane the transformed configuration may be transformed by a general symmetry transformation into any configuration congruent to the given configuration. Hence,

A plane s being given, every displacement in space may be effected by a reflection in s followed by a symmetry transformation.[*]

---

[*] This theorem is due to Study; *l. c.*, p. 497.

If we take s as the plane of a given plane figure we see that *every displacement of a plane figure can be effected by a symmetry transformation.* It is now necessary to study the properties of a symmetry transformation.

The methods employed in the investigation of the product of two reflections in lines show that the effect of combining two reflections in the planes s_1 and s_2 is:

1° A rotation when s_1 and s_2 intersect.

2° A reflection in a line when s_1 and s_2 are perpendicular.

3° A translation when s_1 and s_2 are parallel.

We see also that the product of a reflection in a plane and a reflection in a line perpendicular to the plane, in either order, is a reflection in their point of intersection. Conversely, we deduce corresponding resolutions.

Wiener's theorem now enables us to resolve any displacement (T) into the product of two transformations of which the first is a reflection in an arbitrary plane s; we thus obtain a form of the general symmetry transformation by means of which we can study its properties. Two cases arise.

1° If (T) be a translation or if the axis of (T) cuts the plane s then we may replace (T) by reflections in two lines t_1 and t_2 such that t_1 shall lie in s. We may now replace (t_1) by a reflection in s followed by a reflection in a plane s_1 which passes through t_1 and is perpendicular to s. The symmetry transformation consists of the product $(s_1 t_2)$.

2° If the axis of (T) is parallel to s then t_1 may be chosen perpendicular to s at O. Since a reflection in a plane is involutory

$$(T) = (t_1 t_2) = (s s t_1 t_2) = (s)\ (t_0 t_2),$$

where (t_0) denotes a reflection in the point O. We may replace (t_0) by a reflection in a line t' passing through O perpendicular to t_2 preceded by a reflection in a plane s' passing through O perpendicular to t'. Then

$$(t_0 t_2) = (s' t' t_2) = (s' t''),$$

where (t'') is a reflection in the common perpendicular to t' and t_2 at their point of intersection. Here the symmetry transformation consists of the product $(s' t'')$. Hence,

Every symmetry transformation may be effected by a reflection in a plane followed by a reflection in a line.

Let (s) be the reflection in a plane and (t) the reflection in a line of any symmetry transformation. (t) may be replaced by the product of two

reflections $(s_1 s_2)$ in perpendicular planes such that the plane s_2 is perpendicular to s. The product $(s s_1)$ is a rotation about an axis perpendicular to s_2 or a translation parallel to s_2 according as the planes s and s_1 intersect or are parallel; the latter may be regarded as a special case of the former. Hence

*Every symmetry transformation may be effected by combining in either order a reflection in a plane and a rotation about an axis perpendicular to the plane of the reflection.**

The plane of the reflection is called the *central plane*, its intersection with the axis of the rotation the *centre* of the transformation. From the last theorem we see at once that

In every symmetry transformation the middle points of the chords joining corresponding points lie in the central plane (and coincide with the centre if the angle of the rotation be π); the planes perpendicular to those chords at their middle points pass through the centre of the transformation (and coincide with the central plane if the angle of the rotation be zero).

If a *plane figure* be transformed by a symmetry transformation it is evident that the points in question will lie on a line if the plane of the figure is perpendicular to the central plane and if the rotation reduces to a translation parallel to the given plane. The planes perpendicular to the chords will pass through the axis of the rotation if the plane of the figure coincides with the central plane.

Since any displacement of a plane figure can be effected by a symmetry transformation the remaining theorems of Chasles under consideration are now evident.

THEOREM III. *If a plane figure be displaced the middle points of the chords joining congruent points lie in a plane, on a line or coincide.*

THEOREM IV. *If a plane figure be displaced the planes perpendicular to the chords joining congruent points at their middle points pass through a point, a line or coincide.*

NEW HAVEN, CONN., APRIL, 1900.

---

* Study ascribes this theorem to Hessel; the preceding theorem is due to Study; *l. c.* pp. 487, 565, and 493.

THE COMPLEX OF AXES OF A CENTRAL QUADRIC SURFACE.

By Edward V. Huntington.

The complex of axes of a quadric surface was first presented by Reye, in 1868, in his *Geometrie der Lage*.*

The analytic equations were first stated by Reye.† A detailed discussion of these (unsymmetrical) equations is given by E. Schilke.‡

Additions to the theory have been made by M. G. Koenigs,§ E. Waelsch‖ and H. E. Timerding.¶

The object of the present paper is to restate as briefly as possible such of the chief results of this small chapter of modern geometry as can be conveniently developed by elementary methods.

1. Definition. *A line through any point, perpendicular to the polar plane of that point with respect to a quadric surface, is called an* axis *of the quadric.*** The point, P, is the *pole* of the axis, and the polar plane of P is the *polar plane* of the axis. The *foot* of the axis is the point where it meets its polar plane. All the axes of a quadric taken together constitute the *complex of axes* (*Axencomplex*) of that quadric.

Every point in space (except the centre and the infinite points on the axes of symmetry) is the pole of only one axis; and since there are ∞^3 points in space, there will be in general not more than ∞^3 axes of any quadric. But there are ∞^4 lines in space; hence it is evident that not every line can be an axis.

Our task is, then, to ascertain what lines are axes and what sort of a figure the entire complex of axes forms in space. We shall confine ourselves to the central quadrics, represented by

$$\frac{x^2}{A} + \frac{y^2}{B} + \frac{z^2}{C} = 1 \qquad (1)$$

---

* See Vortrag XV, Vol. 2, of the third edition (1892).

† *Annali di Matematica*, Ser. 2, Vol 2, p. 1–12 (1868–69).

‡ *Zeitschrift für Math. u. Phys.* (*Schlömilch*), Vol. 19, p. 550–564 (1874).

‖ *Nouvelles Annales de Math.*, Ser. 3, Vol. 2, p. 267–272 (1883).

§ *Wiener Sitzungsberichte*, Vol. 95, 2. Abth., p. 549–578 (1887).

¶ *Annali di Matematica*, Ser. 3, Vol. 2, p. 239–261 (1899).

**For another definition see Theorem XIV.

Since the surfaces of revolution possess no interest in this connection, we shall assume that A, B, and C are all different. (*Cf.* Prob. 1.)

We add for reference the familiar equation of the polar plane of any point (x_1, y_1, z_1) with respect to (1):

$$\frac{x_1 x}{A} + \frac{y_1 y}{B} + \frac{z_1 z}{C} = 1. \tag{2}$$

I. The Axes, with their Poles.

2. Some of the lines which belong to the complex may be discovered at once from geometrical considerations.

Thus, if the point P is taken on the quadric, its polar plane coincides with the tangent plane at P and the corresponding axis is perpendicular to the tangent plane at that point. Hence,

Theorem I. *Every normal to the quadric is an axis, having its foot as pole.*

Again, if P is taken at the centre, its polar plane becomes the plane at infinity, to which all lines through the centre are perpendicular. Hence,

Theorem II. *Every diameter of the quadric is an axis, having the centre as pole.*

Again, if P recedes to infinity in the direction of one of the axes of symmetry, its polar plane becomes the plane of symmetry perpendicular to that axis. Hence,

Theorem III. *Every line perpendicular to a plane of symmetry is an axis, having its infinitely distant point as pole.*

We may show, further:

Theorem IV. *Every line lying in a plane of symmetry is an axis.*

For, let a be any line in a plane of symmetry, and let k be the conic section in which the plane cuts the quadric surface.

Now the polar plane of any point in the plane of symmetry with respect to the quadric will be perpendicular to the plane of symmetry, and its trace in that plane will be the polar of the point with respect to the conic section k.

Through the pole Q of a with respect to k draw a line c perpendicular to a. The pole P of c with respect to k will lie on a (since c passes through the pole of a); and the polar plane of P with respect to the quadric will contain c and be perpendicular to a.

Therefore, a is an axis of the quadric; P is its pole, and c is the trace of its polar plane. The theorem is thus established.

We have thus far tacitly assumed that every axis has but a single pole; and it is not hard to show that this is in general the fact. Only in the case of an axis of symmetry, the polar plane of *any* point on the axis is perpendicular to the axis. Hence,

THEOREM V. *The pole of an axis of symmetry is indeterminate.*

3. Let us now find the general condition under which any given line

$$\frac{x-\xi}{l}=\frac{y-\eta}{m}=\frac{z-\zeta}{n} \tag{3}$$

shall be an axis of the surface (1).

Suppose that the line (3) is an axis, and let P_1 (x_1, y_1, z_1) be its pole. Then, since P_1 must lie on the line (3),

$$\frac{x_1-\xi}{l}=\frac{y_1-\eta}{m}=\frac{z_1-\zeta}{n}; \tag{4}$$

and since (3) must be perpendicular to the polar plane (2) of P_1,

$$\frac{x_1}{Al}=\frac{y_1}{Bm}=\frac{z_1}{Cn}. \tag{5}$$

Eliminating x_1, y_1, z_1 from these four equations, we find

$$(B-C)\frac{\xi}{l}+(C-A)\frac{\eta}{m}+(A-B)\frac{\zeta}{n}=0, \tag{6}$$

as the condition under which the line (3) is an axis of the quadric (1).

The equations of the present article give us readily the analytic proof for Theorems II–V (including the statement that every axis except the axes of symmetry has a single determinate pole), and also lead at once to the important theorems of the two following articles.

4. Suppose the direction cosines l, m, n of an axis (3) are given; then the coordinates (ξ, η, ζ) of any point of the axis must satisfy (6), and the coordinates (x_1, y_1, z_1) of the pole of the axis must satisfy (5). These equations are all of the first degree in the variables, and lack a constant term. (The only troublesome case occurs when two of the given cosines are 0, which is the case already considered in Th. III.) Hence,

THEOREM VI. *All axes parallel to a given direction (except those perpendicular to a plane of symmetry) lie in a diametral plane, and their poles lie in a diameter.* (*Cf.* Prob. 7.)

5. Suppose, on the other hand, that a point (ξ, η, ζ) of the axis (3) is given; then the direction cosines l, m, n of the axis must satisfy (6), and the coordinates (x_1, y_1, z_1) of the pole of the axis must satisfy (4) and (5).

Dividing each term of (6) by one of the equal fractions in (3), we have

$$(B-C)\frac{\xi}{x-\xi}+(C-A)\frac{\eta}{y-\eta}+(A-B)\frac{\zeta}{z-\zeta}=0, \tag{7}$$

for the locus of all the axes that pass through the given point (ξ, η, ζ).

And similarly, dividing each term in (4) by one of the equal fractions in (5), we have, dropping the subscripts,

$$A\frac{x-\xi}{x}=B\frac{y-\eta}{y}=C\frac{z-\zeta}{z}, \tag{8}$$

for the locus of the poles of these axes.

We proceed to investigate the nature of both of these loci.

Examining the first of the equations, we see at once that (7) represents a cone of the second degree, with its vertex at the given point (ξ, η, ζ); it contains the diameter through the given point (*cf.* Th. II), and the lines $x=\xi, y=\eta$; $y=\eta, z=\zeta$; and $z=\zeta, x=\xi$ (*cf.* Th. III); and is called the *cone of axes* (*Axenkegel*) of the given point.

Since the cone contains a set of three mutually perpendicular generators it will be an *equilateral* cone, containing an infinite number of such sets.

The second locus, (8), is a space curve containing the poles of all axes through the given point, and therefore called the *pole-curve* (*Polcurve*) of that point.

To determine the order of the curve, set each of the equal fractions in (8) equal to a variable λ; we have then

$$x=\frac{A\xi}{A-\lambda}, \quad y=\frac{B\eta}{B-\lambda}, \quad z=\frac{C\zeta}{C-\lambda}, \tag{8a}$$

as the coordinates of any point of the pole-curve, in terms of the parameter λ. Substituting these values in the equation of any plane, $ax+by+cz+d=0$. we obtain a cubic equation for λ; and to each of the three values of λ thus

determined corresponds one point of intersection of the curve with the plane. In other words, the curve is of the third order.

It is obvious that the pole-curve must lie wholly on the cone of axes; and this appears analytically from the fact that the coordinates (8*a*) of any point of the pole-curve satisfy identically equation (7).

The curve contains the centre (*cf.* Th. II), and the points at infinity on the lines $x=\xi,\ y=\eta$; $y=\eta,\ z=\zeta$; and $z=\zeta,\ x=\xi$ (*cf.* Th. III).

The results of this article may be stated as

THEOREM VII. *All axes through a given point lie on an equilateral quadric cone, having its vertex at the given point, and containing, besides the diameter through that point, the perpendiculars from that point to the planes of symmetry; and their poles form on this cone a space curve of the third order, passing through the given point, and containing, besides the centre, the points at infinity on the perpendiculars to the planes of symmetry.* (*Cf.* Prob. 5.)

6. A simple special case of Th. VII occurs when the given point is taken in a plane of symmetry.

Thus, if the point is $(\xi, \eta, 0)$, the cone (7) breaks up into the plane $z=0$ (*cf.* Th. IV), and the plane $\xi(B-C)(y-\eta)+\eta(C-A)(x-\xi)=0$, which is perpendicular to $z=0$; while the curve (8) breaks up into the equilateral hyperbola $(A-B)xy+B\eta x-A\xi y=0$ in the plane $z=0$, and the straight line $(A-C)x=A\xi$, $(B-C)y=B\eta$, perpendicular to that plane. Hence,

COR. I. *All axes lying in a plane of symmetry and passing through a given point (not in an axis of symmetry) have their poles on an equilateral hyperbola, which contains the given point and the centre, and has asymptotes parallel to the axes of symmetry in that plane.*

COR. II. *All axes that pierce a plane of symmetry in a given point (not in an axis of symmetry) lie in a plane perpendicular to the plane of symmetry; and their poles lie in a straight line, also perpendicular to the plane of symmetry.* (*Cf.* Prob. 6.)

7. The equations of the axis whose pole is the given point (x_1, y_1, z_1) are

$$A\frac{x-x_1}{x_1}=B\frac{y-y_1}{y_1}=C\frac{z-z_1}{z_1}; \tag{9}$$

for, this line (9) contains the given point, and is perpendicular to the polar plane (2) of that point.

8. Two theorems follow immediately from these equations.

Thus, we know that the common value of the equal fractions in (9) is proportional to the distance along the line from the fixed pole to the variable point (x, y, z). Putting successfully $x=0$, $y=0$, $z=0$, we find the distances along the line from the pole to the three coordinate planes are proportional to $-A, -B, -C$. Hence,

THEOREM VIII. *The pole of an axis divides in a constant ratio the portion of the axis intercepted between two planes of symmetry.*

Again, we find that the values of x in (9) corresponding to $y=0$ and $z=0$ are in the ratio $A-B : A-C$. Hence,

THEOREM IX. *The distances from one plane of symmetry to the points where any axis cuts the other two, stand in a constant ratio.*

9. These two theorems enable us to state the following construction:

THEOREM X. *If the three planes of symmetry and any one axis (not perpendicular to or lying in a plane of symmetry), with its pole, are given, then all the other axes of the complex are determined, and can be constructed.*

Thus: from the points where the given axis cuts the planes XY and XZ draw perpendiculars g and h to OX, and determine the ratio of the intercepts, $Og : Oh$.

If we now draw any line g' in XY, perpendicular to OX, and construct the line h' in XZ, perpendicular to OX, such that $Og' : Oh' = Og : Oh$, then all lines that meet both g' and h' will be axes, by Th. IX.

Thus all the axes that pierce any quadrant of the XY plane can be constructed. To these we must add all diameters and all lines perpendicular to or lying in a plane of symmetry (Th. II, III, IV), and the complex is complete.

If the pole of the given axis is known, the poles of all the other axes can be found by Th. VIII. (*Cf.* also, Th. VII, Cor. II.)

II. THE AXES, WITH THEIR POLAR PLANES.

10. If (x_1, y_1, z_1) is the pole of an axis, then its polar plane is given by equation (2).

Now when the axis is made to pass through a fixed point, the coordinates of its pole are given in (8*a*); substituting these values for x_1, y_1, z_1 in (2), we have:

$$\frac{\xi x}{A-\lambda} + \frac{\eta y}{B-\lambda} + \frac{\zeta z}{C-\lambda} = 1, \tag{10}$$

(where λ is a variable parameter) as the equation of the polar plane of any axis passing through the given point (ξ, η, ζ).

This plane (10) is evidently the polar plane of the given point (ξ, η, ζ) with respect to the quadric whose equation is:

$$\frac{x^2}{A-\lambda} + \frac{y^2}{B-\lambda} + \frac{z^2}{C-\lambda} = 1, \tag{11}$$

and we know that this equation represents a family of quadrics confocal to the given quadric (1), their principal sections being confocal conics. Hence,

THEOREM XI. *The polar planes of axes through a given point are the polar planes of that point with respect to a family of quadrics confocal to the given quadric.*

It is shown in the theory of confocal quadrics that three of these surfaces pass through any given point, and cut orthogonally at that point.

Consider then, the three confocal quadrics that contain the given point (ξ, η, ζ); the polar planes of (ξ, η, ζ) with respect to these three surfaces will be the three mutually perpendicular tangent places at that point; and the axes to which these polar planes belong are therefore the three normals to the confocal quadrics at the given point. Hence,

COR. I. *Every point in space is the foot of three axes, which meet at right angles at that point.*

11. It is shown, further, that if from any point P tangents are drawn to the quadric, the axes of symmetry of the cone thus formed are normals to the three confocal quadrics that pass through P. Hence,

COR. II. *The axes of symmetry of any circumscribing cone are axes of the quadric, the foot of each coinciding with the vertex of the cone.*

12. If $\lambda = A$, in the equation (11) of a family of confocal quadrics, the quadric becomes the conic section

$$x = 0, \qquad \frac{y^2}{B-A} + \frac{z^2}{C-A} = 1; \tag{12}$$

and when $\lambda = B$ and $\lambda = C$, we obtain corresponding curves in the planes $y = 0$, $z = 0$, their equations being found by advancing the letters.

These three curves, which belong to the family of confocal quadrics, are called the *focal curves* of that family.

Now when $x = 0$ in the equations of an axis (9), we have the point

$$x=0, \quad y=\frac{B-A}{B}y_1, \quad z=\frac{C-A}{C}z_1;$$

and when $x=0$ in the equation (2) of the polar plane of that axis, we have the line

$$x=0, \quad \frac{y_1 y}{B}+\frac{z_1 z}{C}=1;$$

and these are evidently pole and polar with respect to the focal curve (12). Hence,

THEOREM XII. *The point where an axis cuts a plane of symmetry, and the line in which its polar plane cuts the same plane of symmetry, are pole and polar with respect to a focal curve of the quadric.*

Let the point P and the line a be pole and polar with respect to a focal curve of the quadric. Then every axis that pierces the given plane at P must be perpendicular to some plane containing a. Hence,

COR. *The feet of all axes that pierce a given plane of symmetry in a given point (not in an axis of symmetry) lie on a circle whose plane is perpendicular to the given plane, and whose diameter is the distance from the given point to its polar line with respect to that focal curve which lies in the given plane.* (*Cf.* Th. VII, Cor. II.)

13. We can now state a second construction for the complex of axes, analogous to that given in Th. X. Thus:

THEOREM XIII. *If one of the focal curves of the quadric is given, all the axes of the complex, with their feet, are determined and can be constructed.*

For, the feet of all the axes that lie in the given plane can be constructed as in Th. IV; and all the axes that pierce the given plane at any point (except the centre) can be constructed, with their feet, by Th. XII, Cor. The only axes that remain are those described in Th. II and Th. III.

III. RECIPROCAL POLARS.

14. We know that, if a point moves in a given plane, its polar plane will revolve about a fixed point. Hence, if a point moves along a given *line* (common to two planes), its polar plane will revolve about a second *line* (joining two points); and conversely, if a plane revolves about a given line, its pole will move along a second line.

Two lines so related are called reciprocal polar lines, or simply, *reciprocal polars;* the polar plane of every point on either contains the other.

The reciprocal polar of any axis will be perpendicular to that axis. For it lies in the polar plane of the axis, and all lines in that plane are perpendicular to the axis.

Conversely, any line a, perpendicular to its reciprocal polar, b, will be an axis. For, a plane containing b and the common perpendicular of a and b will be perpendicular to a, and its pole will lie on a; hence, a is an axis.

In the synthetic treatment of the complex of axes, this property is conveniently used as the definition of an axis; thus:

THEOREM XIV. *A necessary and sufficient condition that a line shall be an axis is that it be perpendicular to its reciprocal polar.*

15. THEOREM XV. *The axes of symmetry of any conic section traced on the quadric are axes of the quadric.**

For, let a be an axis of symmetry of such a conic. The tangent planes to the quadric at the extremities of a will contain the parallel tangent lines to the conic at these points; hence the line of intersection of these tangent planes, which is the reciprocal polar of a, will be parallel to both the tangent lines, and therefore perpendicular to a. Thus a is an axis, by Th. XIV.

16. THEOREM XVI. *If two axes lie in a plane, the line joining their poles is also an axis.*

For, the polar planes of each of the poles, P, P', will be perpendicular to the corresponding axis, and hence to the plane, α, in which the axes lie. The line of intersection of these polar planes, which is the reciprocal polar of PP', will then be perpendicular to α, and hence to the line PP' which lies in α. Therefore PP' is an axis, by Th. XIV.

The present theorem may also be stated thus: *All chords of the pole-curve of any point* (Th. VII) *are axes of the quadric.*

COR. I. *The line joining the feet of any two normals that lie in the same plane is an axis of the quadric.*

17. THEOREM XVII. *The product of the distances from the poles of two reciprocal polar axes from a plane of symmetry is constant.*

An outline of the analytic proof for this theorem is as follows.

The axis whose pole is P_1 (x_1, y_1, z_1) is represented by (9), and its reciprocal polar will be the intersection of the polar planes of any two points whose coordinates satisfy (9).

---

*It was from this point of view that the axes were first studied; *cf.* Th. XI, Cor. II.

Selecting the points (x_1, y_1, z_1) and $(x_1/A + x_1, y_1/B + y_1, z_1/C + z_1)$ of the line (9), we can use

$$\frac{x_1 x}{A} + \frac{y_1 y}{B} + \frac{z_1 z}{C} = 1, \qquad \frac{x_1 x}{A^2} + \frac{y_1 y}{B^2} + \frac{z_1 z}{C^2} = 0$$

as the equations of the reciprocal polar axis.

Let P_2 be the pole of this axis. Then P_2 must lie on the axis and the polar plane of P_2 must be perpendicular to the axis, and hence to both the planes which determine the axis. Hence,

$$\frac{x_1 x_2}{A} + \frac{y_1 y_2}{B} + \frac{z_1 z_2}{C} = 1, \quad \frac{x_1 x_2}{A^2} + \frac{y_1 y_2}{B^2} + \frac{z_1 z_2}{C^2} = 0, \quad \frac{x_1 x_2}{A^3} + \frac{y_1 y_2}{B^3} + \frac{z_1 z_2}{C^3} = 0.$$

Solving these three linear equations for x_1x_2, y_1y_2, z_1z_2, we find,

$$x_1 x_2 = a, \quad y_1 y_2 = b, \quad z_1 z_2 = c; \tag{13}$$

where

$$a = \frac{A^3}{(A-B)(A-C)}, \quad b = \frac{B^3}{(B-C)(B-A)}, \quad c = \frac{C^3}{(C-A)(C-B)}.$$

18. The following corollaries follow at once from (13).

Given, the poles of two reciprocal polar axes; then:

Cor. I. *If one moves in a plane parallel to a plane of symmetry, the other will move in a parallel plane.*

Cor. II. *If one moves in a plane containing an axis of symmetry, the other will move in a plane containing the same axis of symmetry.*

Cor. III. *If one moves in any diametral plane, the other will in general move in a quadric cone.*

Cor. IV. *If one moves in any plane whatever, the other will move in general in a surface of the third degree.*

Cor. V. *If one moves in a diameter, the other will move in a diameter.*

Cor. VI. *If one moves in a line parallel to a principal axis, the other will move in a parallel line.*

IV. Coaxial Quadrics.

19. In conclusion, let us see what changes in the given quadric (1) can be made without disturbing the complex of axes of that quadric; in other words, let us see whether the same complex may not belong to more than one quadric.

The condition (6), under which a given line is an axis of the quadric (1), remains unaltered when we add any constant to A, B, and C, or when we multiply A, B, and C by any constant factor.

That is, any line which is an axis of (1) will be also an axis of the quadric represented by

$$\frac{x^2}{A-\lambda}+\frac{y^2}{B-\lambda}+\frac{z^2}{C-\lambda}=\mu \qquad (14)$$

whatever the values of the constants λ and μ.

This equation contains two arbitrary parameters, and therefore represents a doubly infinite series of quadrics.

If λ alone varies, while $\mu=1$, we have a family of quadrics confocal to (1).

If, for any given value of λ, μ is allowed to vary, we have a family of quadrics similar, concentric, and similarly placed to the quadric which corresponds to the given value of λ. If we use the word *concyclic* to describe quadrics that are similar, concentric, and similarly placed, we have the theorem:

THEOREM XVIII. *All the quadrics of a confocal family with all the quadrics concyclic to each of these quadrics have the same complex of axes.*

The quadrics represented by (14) have therefore been called by Reye *coaxial*. All coaxial quadrics have the same axes, but these axes do not in general have the same poles and the same feet with respect to all the quadrics.

If $\lambda=0$, and only μ be allowed to vary, then not only the condition (6), but also the locus (9) of the poles of axes through a given point, will remain unaltered. Hence,

COR. I. *All concyclic quadrics not only have the same complex of axes, but each axis preserves its own pole.*

If $\mu=1$, and only λ be allowed to vary, we have a family of confocal quadrics, which is wholly determined if one of its focal curves is known. Hence, by Th. XIII,

COR. II. *All confocal quadrics not only have the same complex of axes, but each axis preserves its own foot.*

MISCELLANEOUS PROBLEMS.

1. If the quadric (1) is a quadric of revolution, the complex of axes is composed of: (a) all lines perpendicular to the axis of rotation; and (b) all

lines meeting that axis or parallel to it. In the case of a sphere, every line in space may be regarded as an axis. (Th. III.)

2. The poles of all axes that meet a given line lie on a quadric surface containing the given line. If the given line is a diameter, the surface becomes a cone containing, besides the given line, the three axes of symmetry.

Let the given line be $ax + by + cz + d = 0, \quad a'x + b'y + c'z + d' = 0.$
From (9) express the coordinates of any point of the axis in terms of a variable parameter. Then

$$\frac{ax + by + cz + d}{\frac{ax}{A} + \frac{by}{B} + \frac{cz}{C}} = \frac{a'x + b'y + c'z + d'}{\frac{a'x}{A} + \frac{b'y}{B} + \frac{c'z}{C}}$$

is the equation of the required quadric.

3. The poles of all axes that meet a plane of symmetry along a line perpendicular to an axis of symmetry lie in a plane perpendicular to that axis. (*Cf.* Th. VII, Cor. II, and Prob. 6, below.)

(Special case of the preceding.)

4. The poles of all axes parallel to a given plane lie in a diametral plane; the poles of all axes in a given plane lie on a line.

Let the given plane be $ax + by + cz + d = 0$; then, using (9),

$$\frac{ax}{A} + \frac{by}{B} + \frac{cz}{C} = 0$$

is the equation of the required diametral plane.

5. The feet of all axes through a given point form on the cone of axes of that point (Th. VII) a space curve of the fifth order,* containing the infinite point of the diameter through the given point, and the feet of the perpendiculars from the given point to the planes of symmetry; and passing three times through the given point.

In this and the following problems on the feet of the axes, it is convenient to use the unsymmetrical equations of a line. Show that the equations

$$x = \frac{y}{m} + h, \quad x = \frac{z}{n} + kh, \qquad \text{where } k = \frac{A - C}{A - B},$$

represent any axis of the quadric (1); find the pole of this axis, and show that

$$x + my + nz = \frac{A - B}{h}$$

is the equation of its polar plane.

---

* This curve has been studied in detail by A. Schmitz: *Programm der K. bayr. Studienanstalt, Neuberg a. D.*, for 1886–87.

Expressing the condition that the axis shall pass through the given point (ξ, η, ζ) and eliminating m, n, and b, we find

$$x(x-\xi)+y(y-\eta)+z(z-\zeta)=(A-B)\frac{(x-\xi)(y-\eta)}{\xi y-\eta x}=(A-C)\frac{(x-\xi)(z-\zeta)}{\xi z-\zeta x}$$

as the equations of the required locus.

6. The feet of all axes through a given point in a plane of symmetry (but not in an axis of symmetry) lie (a) in a curve of the third order in that plane; and (b) in a circle perpendicular to that plane and bisected by it. (*Cf.* Th. VII, Cor. I, II.)

(Special case of the preceding.)

7. The feet of all axes parallel to a given direction (except those perpendicular to a plane of symmetry) lie in an equilateral hyperbola. (*Cf.* Th. VI.)

(Special case of Prob. 5 when the given point recedes to infinity in a given direction. There is also a curve of the third order, lying wholly at infinity, that belongs to the locus.)

8. The feet of all axes that meet a plane of symmetry along a line perpendicular to an axis of symmetry lie on a surface of the third order. The surface has two planes of symmetry and contains two families of circles; it is a special case of the Cyclide of Dupin. (*Cf.* Th. XII, Cor., and Prob. 3.)

If the given line is $y=0$, $x=b$, then

$$x+\frac{y^2}{x-b}+\frac{z^2}{x-kb}=\frac{A-B}{b}, \qquad \text{where } k=\frac{A-C}{A-B},$$

is the equation of the surface.

9. The six normals that can be drawn from a given point to a quadric surface lie on an equilateral quadric cone, containing, besides the diameter through that point, the perpendiculars from that point to the three planes of symmetry; and their feet lie on a space curve of the third order, containing, besides the centre and the given point, the points at infinity on the perpendiculars to the planes of symmetry. (Th. I, Th. VII.) (Steiner.)

10. Through any given point an infinite number of coaxial central quadrics can be passed. Their normals at this point lie on a quadric cone.

11. The polar planes of a given point with respect to a family of concyclic quadrics are parallel. (Th. XVIII, Cor. I.)

12. The poles of a given plane with respect to a family of confocal quadrics lie in a line perpendicular to that plane. (Th. XVIII, Cor. II.)

13. A given plane cuts a family of confocal quadrics in a series of conic sections whose axes of symmetry are tangent to a fixed parabola and whose

centres lie on a fixed line; this line is the directrix of the parabola; it passes through the foot of the perpendicular from the centre on the given plane, and through the foot of the perpendicular (Prob. 12) in which lie the poles of the given plane with respect to the quadrics.

14. All axes in a given plane envelop a parabola; their poles lie on a line tangent to the parabola; and their feet lie on a curve of the third order. The pole of this line with respect to the conic in which the given plane cuts the surface is a double point of the curve.

15. Discuss the complex of axes of a paraboloid.

STRASSBURG, GERMANY, JANUARY, 1900.

GALOIS' THEORY OF ALGEBRAIC EQUATIONS.

PART II. IRRATIONAL RESOLVENTS.

By James Pierpont.

Introduction.

In Part I the reader has gained an *aperçu* of the essential features of Galois' Theory. To make this as easy as possible all details were left aside; furthermore, only *rational resolvents* were considered. In the present paper we complete our account of Galois' Theory by 1° showing that all the steps required by Galois' theory can actually be performed; 2° by developing some of the consequences which follow when we make use of *irrational resolvents*.

The importance of the second topic can already be seen. In §31 we established a *sufficient* condition in order that an equation $f(x) = 0$ can be solved algebraically. Is this condition necessary? The reasoning employed in Part I can never answer this question, for all the auxiliary equations there employed were *rational resolvents*; *i. e.*, equations whose roots were rational functions of the roots of the given equation $f(x) = 0$. To show that our condition is not only sufficient but also *necessary* we must study the effect of adjoining roots of equations which are not rational in the roots of $f = 0$. Such equations are called *irrational resolvents*. The theory of irrational resolvents enables us not only to answer this important question, but is also of fundamental importance in many other investigations.

Consider now the first topic. This will not appeal to all readers alike. We show, indeed, that every step required by Galois' theory in the solution of a given equation can actually be performed. But such solutions will seem very illusory to some readers when they reflect how tremendous the calculations are, even when every known device is employed to shorten them. To this we reply twofold: First, the length of the calculations is not at all peculiar to our theory. Consider *e. g.* the corresponding problems in the theory of Partial Differential Equations or the calculations that certain astronomical problems of to-day require. Secondly, we can take a higher standpoint. We can say that a mathematical theory takes an immense step in advance when its *logical* definitions are replaced by those which enable us actually to

find or decide what we are defining. Such definitions afford us a far deeper insight into the nature of the quantities or objects they involve.

All Operations Required in Galois' Theory can be Performed.

37. Statement of the Three Remaining Problems. The scheme for solving a given equation as developed in Part I required: the determination of the Galoisian Group, the determination of its subgroups, and the construction of rational functions of the roots belonging to these subgroups. In §19 the determination of the Galoisian group was reduced to the determination of the irreducible factors of the Galoisian Resolvent. In §18 the construction of rational functions of the roots belonging to a given group was reduced to the problem of deciding whether two rational functions of the roots are equal or not.

We have, then, three problems before us if we wish to show that all steps required in Galois' theory can actually be performed, viz.:

Problem A. *To determine all the subgroups of a given substitution group.*

Problem B. *To determine whether two rational functions of the roots of the given equation are distinct or not.*

Problem C. *Reduction of an integral rational function of one variable into irreducible factors for an arbitrary domain.*

In solving these problems our aim will not be to effect the solution in the most expeditious manner, but merely to show that each can be solved by a finite number — easily determined in advance — of operations each of which can be actually executed.

38. Problem A. This is easily disposed of. Let G be the given substitution group. All its subgroups may be found thus. Take at random a set S of substitutions in G, say $\alpha, \beta, \gamma \ldots$. Form all products of pairs $\alpha\beta, \alpha\gamma, \beta\gamma, \ldots$. If these lie in S, S is a subgroup; otherwise not. As there are only a finite number of sets S, these can be written down and examined. The sets S which we have actually to consider in any given case can be limited to a large extent. Thus: in each set the identical substitution must be present; again if α is in S, so are $\alpha^2, \alpha^3, \ldots$; and finally, the number of substitutions taken in S must be a divisor of the order of G, etc., etc.

39. Canonical Form of a Domain. Before taking up Problem B it will be convenient to find a simple form to which any domain R may be reduced. Our domains as we saw §2 consisted of certain quantities $q_1, q_2 \ldots$

and algebraic functions built up on them. The q's that are transcendental constants can be replaced by indeterminates without altering the character of our results. Thus without loss of generality we can suppose the q's are variables. The algebraic functions in R may be obtained progressively as follows. The first lot will be roots of algebraic equations

$$f_1 = 0, \qquad f_2 = 0, \qquad f_3 = 0, \ldots . \tag{1}$$

whose coefficients lie in $Q(q_1, q_2 \ldots)$.
Let their roots be

$$x_1, x_2, \ldots . ; \; y_1, y_2, \ldots . ; \; z_1, z_2, \ldots . . . . . ; \ldots . \tag{2}$$

We can suppose that only one root is taken from each equation (1); for if several lay in R, we can suppose the equation repeated in (1) as many times as we take roots from it. Furthermore we can suppose the equations (1) are irreducible for Q. Say the roots we need to take for our first step are $x, y, z, \ldots$ Form the rational function

$$\xi = ux + vy + wz + \ldots . \tag{3}$$

where $u, v, w, \ldots$ are indeterminates. In (3) replace $x, y, z, \ldots$ by all possible sets taken from (2), and let ξ go over into $\xi_1, \xi_2, \ldots .$ The equation

$$F(t) = (t-\xi)(t-\xi_1)(t-\xi_2) \ldots . = 0$$

is evidently rational for Q, since its coefficients are symmetric functions of the roots of (1).

We show now that the domains $T(Q, x, y, z, \ldots .)$ and $T'(Q, \xi)$ are identical. For evidently T' lies in T, since every rational function of ξ is a rational function of $x, y, z, \ldots .$ Conversely T lies in T'. For let $\phi(x, y, z, \ldots)$ be any quantity in R and let ϕ go over into $\phi_1, \phi_2, \ldots .$ for the substitutions which converted ξ into $\xi_1, \xi_2, \ldots .$ Consider the function

$$G(t) = F(t) \left\{ \frac{\phi}{t-\xi} + \frac{\phi_1}{t-\xi_1} + \ldots . \right\}.$$

Being symmetrical in the roots of (1) its coefficients lie in Q. It is therefore a rational polynomial in t. For $t = \xi$ it gives

$$G(\xi) = \phi \, F'(\xi), \tag{4}$$

where $F'(t)$ is the derivative of $F(t)$, $\therefore$ ϕ lies in T'.

From this point all new algebraic functions which we need to adjoin to get R can be taken one at a time. The general case is this: We have a current domain

$X(\xi, Q)$ which we enlarge to $Y(\eta, X)$, by adjoining to X a root η of an irreducible rational equation for X, say $h(t, \xi) = 0$. The algebraic function ξ is root of an irreducible equation; say $F(t, Q) = 0$ for Q. To reduce this case to the preceding, form the product

$$H(t) = h(t, \xi)\, h(t, \xi_1)\, h(t, \xi_2) \ldots .$$

extending over all the conjugate roots to ξ. Evidently the coefficients of H lie in Q. Let $k(t, Q)$ be the irreducible factor which vanishes for $t = \eta$. Evidently now the domain Y may be generated by adjoining to Q a root of each of the equations $F(t, Q) = 0$, $k(t, Q) = 0$. We have thus the

THEOREM. *Every domain of rationality may be regarded as generated by a certain number of variables or indeterminates $q_1, q_2 \ldots$ and a single root ξ of an equation rational and irreducible for the domain $Q(q_1, q_2, \ldots)$.*

Definition. When a domain $R(\xi, q_1, q_2, \ldots)$ is considered as generated by a single algebraic function of certain variables $q_1, q_2, \ldots$ it is also called a *body* (*Körper*).

Definition. Let $f(\xi)$ be a quantity in $R(\xi)$, the product $Nf = f(\xi) f(\xi_1) f(\xi_2) \ldots$ extended over all conjugate roots of ξ is called the *norm* of f. Evidently if $f = gh$, $Nf = Ng \cdot Nh$.

Definition. If the degree of the irreducible equation for $Q(q_1, q_2, \ldots)$ which ξ satisfies is m, the *order* of R is m.

With any quantity η lying in R, we can generate a domain $S(\eta, q_1, q_2, \ldots)$ which, lying entirely in R, is called an *inferior body* of R (*Unterkörper*); also a *subdomain*. We can call R a *superior body* of S (*Oberkörper*); also *superior domain*.*

40. Problem B. We have to determine whether the two rational functions

$$\phi(x_1, x_2, \ldots ; q_1, q_2, \ldots, \xi), \qquad \psi(x_1, x_2, \ldots ; q_1, q_2, \ldots, \xi)$$

are equal or not. Here $x_1, x_2 \ldots$ are roots of the given equation $f(x) = 0$,

* The reasoning employed to deduce (4) enables us to justify a tacit assumption made §12,1°. We assumed there that $\phi(x_1, x_2, \ldots) = \psi(V_1) = \psi(V_2) = \ldots = \psi(V_m)$ because $\phi(x_1, x_2, \ldots)$ remained unaltered for the substitutions (3), §12. That this is indeed so we can now easily show. In fact, take for $\xi, \xi_1, \xi_2, \ldots$ above, $V_1, V_2, \ldots V_m$; then

$$\phi_i = \frac{G(V_i)}{F'(V_i)} = r_0 + r_1 V_i + \ldots + r_{m-1} V_i^{m-1}, \qquad i = 1, 2 \ldots m.$$

Here the r's are the same for all i. This shows that in (4) §12, the m substitutions (3) can be effected and the resulting equations are correct.

and the domain is $R(\xi, q_1, q_2 \ldots)$. Let the Galoisian Resolvent $G = 0$ be of degree m, then by §11, (3) we have

$$\phi = r_0 + r_1 V + \ldots + r_{m-1} V^{m-1}; \qquad \psi = s_0 + s_1 V + \ldots + s_{m-1} V^{m-1}.$$

In order that $\phi = \psi$ it is necessary and sufficient that $r_\kappa = s_\kappa$, $\kappa = 0, 1, \ldots m-1$. For, $\phi - \psi = 0$ is a rational equation in V of degree $< m$ and this is impossible, since $G = 0$ is irreducible, unless $r_\kappa - s_\kappa = 0$.

The question is thus reduced to decide whether two rational functions of ξ for $Q(q_1, q_2, \ldots)$ are equal or not. Repeating the reasoning for ξ that we have just made for V, the question becomes this: To decide whether two integral rational functions for $R(1)$, viz.

$$L(q_1, q_2 \ldots), \quad M(q_1, q_2 \ldots)$$

of the independent variables $q_1, q_2 \ldots$ are equal or not. This problem is no more difficult if, instead of $R(1)$, we take any other domain S containing only constants.

Let us begin with a single variable. The integral rational function

$$G(q_1) = a_0 q_1^n + a_1 q_1^{n-1} + \ldots + a_n,$$

the a's being constants, can vanish but n times unless the a's are all zero, when it vanishes identically. Observe that we can therefore give q_1 an infinity of values, integral values for example, for which $G \neq 0$.

Pass now to two variables q_1, q_2. Let $G(q_1, q_2)$ be of degree n_1 in q_1 and of degree n_2 in q_2. We can write it,

$$G(q_1, q_2) = q_2^{n_2} g_0(q_1) + q_2^{n_2-1} g_1(q_1) + \cdots + g_{n_2}(q_1).$$

Here we can choose q_1 in an infinity of ways so that all the g's are $\neq 0$ unless the g's are identically zero. Let $q_1 = a$ be such a value. We can choose q_2 in an infinity of ways so that $G(a, q_2) \neq 0$. Hence we can choose the variables q_1, q_2 in an infinity of ways, choosing even integers, so that $G \neq 0$. $G(q_1, q_2)$ cannot $= 0$ in the sense of §5 unless all the coefficients of q_1, q_2 are zero.

The generalization to n variables is evident, giving the following theorems.

THEOREM I. *Being given any finite number of rational integral functions of the independent variables* $q_1, q_2, \ldots,$

$$G(q_1, q_2, \ldots), \quad H(q_1, q_2, \ldots), \ldots$$

the coefficients of no one of which are all zero, it is possible to choose the variables in an infinity of ways — taking even integral values — so that none of the functions vanish.

This shows that the $n!$ valued function of §8 can be constructed.

THEOREM II. *If the integral rational function $G(q_1, q_2, \ldots)$ with constant coefficients vanish in the sense of §5, all its coefficients must be zero.*

Since $F = G$ is equivalent to $F - G = 0$ we have also

THEOREM III. *If two integral rational functions $F(q_1, q_2 \ldots)$, $G(q_1, q_2, \ldots)$ with constant coefficients are equal, it is necessary and sufficient that the coefficients of like terms in F and G are equal, i. e. F and G must be formally equal.*

41. Lagrange's Formula of Interpolation. In this connection let us show how an integral rational function $F(q_0, q_1, \ldots q_n)$ of $n+1$ variables and of degree n_0 in q_0 is known when its values $f_\kappa(q_1, q_2 \ldots q_n)$ are known for $n_0 + 1$ distinct values of q_0, say for $q_0 = a_0, a_1, \ldots a_{n_0}$. We shall need this in Problem C. We set

$$L_\kappa(q_0) = (q_0 - a_0) \ldots (q_0 - a_{\kappa-1})(q_0 - a_{\kappa+1}) \ldots (q_0 - a_n), \quad \kappa = 0, 1, \ldots n_0.$$

Evidently $L_\kappa \neq 0$ for $q_0 = a_\kappa$ while $L_\kappa = 0$ for the other a's. Consider now the function

$$\Phi(q_0, q_1, \ldots q_n) = \sum_\kappa f_i(q_1, \ldots q_n) \frac{L_\kappa(q_0)}{L_\kappa(a_\kappa)} \tag{1}$$

Evidently $\Phi(a_i, q_1, q_2, \ldots q_n) = f_i(q_1, \ldots q_n), \qquad i = 0, 1, \ldots n_0.$

Hence by §40, $\Phi = F$. The right side of (1) is called Lagrange's Formula of Interpolation.

42. Uniqueness of the Decomposition of an Integral Function into Irreducible Factors for R (1). We turn now to Problem C. We consider first the decomposition of integral rational functions with integral coefficients for R (1). This problem we break up into two parts. We show first that the decomposition is *unique*, and then show how the irreducible factors may be actually found.

For brevity we shall call in this and the following § integral rational functions with integral coefficients *integral functions*. We wish to prove the

THEOREM: *An integral function can be decomposed in but one way into irreducible factors for R (1).*

Our method is that of complete induction. Let us recall, therefore, how the corresponding theorem is proved for integers. The demonstration rests essentially on the Euclidian algorithm of the greatest common divisor. In fact, this algorithm gives at once:

(*a*) *If F, G be two integers which are relatively prime, then there exist two integers A, B for which*

$$AF + BG = 1. \tag{1}$$

From this we conclude:

(*b*) *If EF is divisible by the prime G and if F is not divisible by G, then E is.*

From (1) it follows that $AEF + BEG = E$. Here the left side is divisible by G since by hypothesis EF is. Hence the right side is.

From this follows easily:

(*c*) *The decomposition of an integer into prime factors is unique.*

For say $F = P_1 P_2 \ldots P_m = Q_1 Q_2 \ldots Q_n$ were two such decompositions. As F is divisible by P_1 the product $Q_1 \cdot Q_2 \ldots Q_n$ is. Hence by (*b*) either Q_1 is divisible by P_1 or $Q_2 \ldots Q_n$ is. If Q_1 is divisible, $Q_1 = P_1$ since P is a prime. We have then established the identity of one of the prime factors in the two decompositions. If Q_1 is not divisible by P_1, then $Q_2 \cdot Q_3 \ldots Q_n$ is, and (*b*) shows that either Q_2 or $Q_3 \ldots Q_n$ is divisible by P_1. Evidently we must finally come to a Q_ϵ which $= P_1$. A repetition of this reasoning on the quotients that remain after P_1 has been divided out establishes the theorem.

We proceed now to prove the analogous theorems to (*a*), (*b*), and (*c*) for integral functions. We shall denote these theorems by *A*, *B*, *C*. We shall frequently need to consider an integral function $F(q_0, q_1, \ldots q_n)$ as a function of one variable, say q_0. We shall indicate this by writing it $F(q_0; q_1, \ldots q_n)$ or more shortly $F(q_0)$. Also, as in arithmetic, we write $F \equiv 0$, mod G, when F is divisible by G; while $F \not\equiv 0$, mod G, indicates that F is not divisible by G. We shall not repeat the modulus except to avoid ambiguity. We must first establish a number of auxiliary theorems.*

THEOREM I. *If the integral function $F(q_0, q_1 \ldots q_n)$ be divisible by an integral function of only n variables $g(q_1, q_2 \ldots q_n)$, then each coefficient of $F(q_0)$ is $\equiv 0$ mod g.*

For

$$F(q_0) = f_0(q_1, \ldots q_n) q_0^{n_0} + f_1(q_1, \ldots q_n) q_0^{n_0-1} + \ldots \tag{1}$$

$$= g(q_1, \ldots q_n) H(q_0, q_1, \ldots q_n)$$

$$= g(q_1, \ldots q_n) \{h_0(q_1, \ldots q_n) q_0^{n_0} + h_1(q_1, \ldots q_n) q_0^{n_0-1} + \ldots\} \tag{2}$$

* The reader will grasp these demonstrations much better if he goes through the reasoning first for the case $n = 1$. He can then extend it to the case $n = 2$. The general case will then give no trouble. This applies also to §41.

The comparison of (1) and (2) gives §40,

$$f_\kappa(q_1, \ldots q_n) = g(q_1, \ldots q_n)\, h_\kappa(q_1, \ldots q_n). \qquad \kappa = 0, 1, \ldots$$

THEOREM II. *If $F(q_0 \ldots q_n)$ and $G(q_0 \ldots q_n)$ be integral functions of $n+1$ variables and if FG be divisible by an integral irreducible function of n variables $g(q_1 \ldots q_n)$, while F is not, then G is divisible by g.*

We suppose Theorem B (stated precisely below) is true for n variables. As we are reasoning from n to $n+1$, this is permissible. We have, assuming that, say, F contains the variable q_0,

$$F(q_0) = a_0 + a_1 q_0 + a_2 q_0^2 + \ldots$$
$$G(q_0) = b_0 + b_1 q_0 + b_2 q_0^2 + \ldots$$

Since $F \not\equiv 0 \bmod f$, at least one of its coefficients is $\not\equiv 0$. Say the first such is a_α. To show $G \equiv 0$, suppose the contrary. Then at least one of its coefficients $\not\equiv 0$; say b_β is the first such.

Then

$$FG \equiv (a_\alpha q_0^\alpha + a_{\alpha+1} q_0^{\alpha+1} + \cdots)(b_\beta q_0^\beta + b_{\beta+1} q_0^{\beta+1} + \cdots)$$
$$\equiv a_\alpha b_\beta q_0^{\alpha+\beta} + \text{terms of higher degree in } q_0.$$

Here by Theorem I every coefficient on the right side is $\equiv 0$, $\therefore a_\alpha b_\beta \equiv 0$, $\therefore$ by Theorem B, $b_\beta \equiv 0$ and this is a contradiction.

THEOREM III. *Let $F(q_0 \ldots q_n)$, $G(q_0 \ldots q_n)$ be integral functions of $n+1$ variables and let G be irreducible. If the quotient F/G can be written*

$$\frac{F}{G} = a_0 + a_1 q_0 + a_2 q_0^2 + \ldots$$

where the a's are RATIONAL *functions of the other variables, then they are also* INTEGRAL.

For the right side can be written

$$\frac{F}{G} = \frac{\alpha_0 + \alpha_1 q_0 + \alpha_2 q_0^2 + \ldots}{\beta}$$

where the α's and β are integral in $q_1, \ldots q_n$ and without common divisor, We have now

$$\beta F = G(\alpha_0 + \alpha_1 q_0 + \ldots) = G \cdot H$$

Here β divides GH, while H is not divisible by a single prime factor of β_0. Applying Theorem II we conclude that β divides G. But G is irreducible $\therefore \beta = 1$.

THEOREM IV. *If the integral function of $n+1$ variables $F(q_0, q_1 \cdots q_n)$ can be split into two factors*

$$F(q_0 \cdots q_1) = G(q_0; q_1 \cdots q_n)\, H(q_0; q_1 \cdots q_n),$$

integral with respect to q_0 and rational in the other variables $q_1, \cdots q_n$, then G and H can be so taken as also to be integral in $q_1, \cdots q_n$.

For clearing of fractions we have

$$F(q_0 \cdots q_n) = \frac{G_1(q_0 \cdots q_n)\, H_1(q_0 \cdots q_n)}{k(q_1 \cdots q_n)}$$

where G_1, H_1, k are integral functions of the variables indicated. We can also suppose G_1 to be irreducible. We have now

$$\frac{F(q_0 \cdots q_n)}{G_1(q_0 \cdots q_n)} = \frac{H_1(q_0 \cdots q_n)}{k(q_1 \cdots q_n)}.$$

The application of Theorem III shows that F is divisible by G_1.

This theorem is the generalization of Gauss' theorem in one variable.

We conclude now at once:

THEOREM V. *The integral functions $F(q_0 \cdots q_n)$, $G(q_0 \cdots q_n)$ are relatively prime or not according as $F(q_0)$, $G(q_0)$ are.*

We are now able to establish

THEOREM A. *If two integral functions $F(q_0 \cdots q_n)$ and $G(q_0 \cdots q_n)$ are relatively prime, there exist two functions $A(q_0 \cdots q_n)$, $B(q_0 \cdots q_n)$ integral with respect to q_0 and rational in $q_1, \cdots q_n$ so that*

$$AF + BG = 1.$$

For the algorithm of the greatest common divisor of $F(q_0)$, $G(q_0)$ determines two functions of just this type.

We can now prove

THEOREM B. *If the product of two integral functions $E(q_0 \cdots q_n)$ $F(q_0 \cdots q_n)$ of $n+1$ variables is divisible by an irreducible integral function $G(q_0 \cdots q_n)$ and if E is not divisible by G, F must be.*

We have assumed this true for n variables; we show now it is true for $n+1$ variables. For $n = 0$ it is Theorem (b).

From Theorem A we have $AE + BG = 1$. Multiply this by E/G. Then

$$\frac{AEF}{G} + BE = \frac{E}{G}$$

Since EF is divisible by G, the left side is integral in q_0 and rational in $q_1, \ldots q_n$. Then Theorem III shows that E is divisible by G.

THEOREM C. *An integral rational function $F(q_0, q_1, \ldots)$ of the independent variables $q_0, q_1 \ldots$ with integral coefficients can be decomposed into irreducible factors for $R(1)$ in only one way.*

This is demonstrated precisely as (c), *ante*.

43. Actual Decomposition of $F(q_0, q_1, \ldots q_n)$ for $R(1)$. We suppose the problem solved for n variables and show how to solve it for $n + 1$. When $n = 0$, we have the decomposition of an integer into prime factors. Suppose F to be of degree m_0 with respect to say q_0. Theorem IV §42 shows that in seeking a divisor $G(q_0, \ldots q_n)$ of F we need consider none of degree higher than $\mu \equiv m_0/2$ in q_0. This restricts the possible form of our divisors somewhat. A far more incisive restriction is obtained from the simple observation that, giving to q_0 an integral value, say $q_0 = a$, $G(a, q_1, \ldots q_n)$ must be a divisor of $F(a, q_1, \ldots q_n)$. But $F(a, q_1, \ldots q_n)$ being a function of only n variables, all its divisors can be found. $G(a, q_1, \ldots q_n)$ must lie among these which are finite in number. With this we combine the fact that the function $G(q_0)$ is known when its values are given for $\mu + 1$ values of q_0 by virtue of Lagrange's Formula.

Let us give then q_0, $\mu + 1$ arbitrary but distinct integral values

$$q_0 = a_0, a_1, \ldots a_\mu,$$

and denote the corresponding divisors of $F(a_\kappa, q_1, \ldots q_n)$ by

$$f'_\kappa, \quad f''_\kappa, \quad f'''_\kappa, \ldots \qquad \kappa = 0, 1, 2 \ldots \mu$$

Then

$$\begin{aligned}
&G(a_0, q_1, \ldots q_n) \text{ must be one of the quantities } f'_0, f''_0, f'''_0 \ldots \\
&G(a_1, q_1, \ldots q_n) \quad \ldots \ldots \ldots \ldots \quad f'_1, f''_1, f'''_1 \ldots \\
&\ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots \\
&G(a_\mu, q_1, \ldots q_n) \quad \ldots \ldots \ldots \ldots \quad f'_\mu, f''_\mu, f'''_\mu \ldots
\end{aligned}$$

That is, the possible values G can have for $\mu + 1$ values are known. Hence G must be sought among the integral functions, finite in number, which take on these values f'_κ for $q_0 = a_0, a_1, \ldots a_\mu$. These are all given by Lagrange's Formula. Thus to decompose F we write down all these *possible* divisors $G_1, G_2, \ldots$ and divide F through by them; if the division comes out without remainder the particular G in question is a divisor, otherwise not.

44. Solution of Problem C. Let $F(t)$ be an integral function of t; we seek to decompose it into irreducible factors for an arbitrary domain

$R(\xi, \eta_1, \eta_2 \ldots)$. The coefficients of t we take as integral functions of $\xi, \eta_1, \ldots$ whose coefficients in turn are integers. It may happen that F does not contain ξ; in this case we introduce an indeterminate u, and replace t by $t + u\xi$. At the close we make the inverse substitution.

Suppose now $F = GH$ for R. Taking the norm we have

$$NF = NG \cdot NH. \tag{1}$$

The functions NF, NG, NH are integral functions of $t, \eta_1, \eta_2 \ldots u$. From (1) we see at once that if NF is irreducible for $R(1)$, F is irreducible for R. From (1) we also conclude that if a divisor G exists, it must be a divisor of NG, *i. e.*, every divisor of F is a common divisor of F and a factor of NF. Hence in order to find possible divisors of F, we find its norm and all the divisors $D_1, D_2, \ldots$ of this norm for $R(1)$. We then seek the greatest common divisor of F and one of these D's by the ordinary method. This takes but a finite number of rational operations.

45. Irreducibility of $x^p - a$. Before leaving the subject of reducibility we prove the following theorem which we shall find useful later, although in no wise an illustration of the foregoing theory.

THEOREM. *If p be a prime and a a quantity in a given domain R which is not the p^{th} power of a quantity in R, then $F(x) = x^p - a$ is irreducible for R.*

For let

$$G(x) = (x - \rho^{e_1}\xi)(x - \rho^{e_2}\xi) \ldots (x - \rho^{e_m}\xi)$$

be a rational factor of F, where ξ is *one* root of F. All the coefficients of G lying in R, the absolute term, that is,

$$\rho^{e_1 + e_2 + \ldots + e_m}\, \xi^m = \rho^e\, \xi^m \tag{1}$$

is in R. Unless $m = p$ it is possible to determine n so that $mn \equiv 1 \bmod p$. Say $mn = 1 + pq$. Raise (1) to the n^{th} power; we get $\rho^{en}\, \xi^{mn} = \rho^{en}\, a^q\, \xi = b$, and this lies in R. Then $\xi = \rho^{-en} a^{-q} b$. Raising this to pth power we have $\xi^p = a = (a^{-q} b)^p$, which asserts that a is the pth power of a quantity in R. Hence $m = p$.

IRRATIONAL RESOLVENTS.

46. Kronecker's Theorem. We turn now to our second topic: the *rôle* irrational resolvents play in the solution of equations. The theorem which lies at the base of the subject is due to Kronecker.

FUNDAMENTAL THEOREM. *Let $f(x) = 0$, $g(y) = 0$ be two rational irreducible equations for the domain R of degrees m, n respectively. If on adjoining a root x_1 of $f = 0$, $g(y)$ becomes reducible, the adjunction of a root y_1 of $g = 0$ will make $f(x)$ reducible. Let $\phi(x)$, $\psi(y)$ of degrees α, β respectively be the irreducible factors for the new domains that x_1, y_1 satisfy, then*

$$m\beta = n\alpha.$$

In fact, let the roots of

$$f(x) = 0, \quad g(y) = 0, \quad \phi(x) = 0, \quad \psi(y) = 0,$$

be respectively

$$x_1, \ldots x_m; \quad y_1, \ldots y_n; \quad x_1, \ldots x_\alpha; \quad y_1, \ldots y_\beta.$$

Let $F(t, u, v)$ be the irreducible factor for R of

$$\Pi(t) = \Pi(t - ux_\iota - vy_\kappa), \qquad \begin{matrix} \iota = 1, 2 \ldots m \\ \kappa = 1, 2 \ldots n. \end{matrix}$$

admitting the root $t = ux_1 + vy_1$. Here u, v are indeterminates. The degree of F call j; we show $j = m\beta$.

To this end observe that $F(t, 1, 0) = 0$ has one solution in common with $f = 0$, hence it has all. Hence the index ι in F runs from 1 to m. Consider now the factors of the form $t - ux_1 - vy_\kappa$ in F. κ must run from 1 to β. For the product

$$G(t, x_1) = \Pi(t - ux_1 - vy_\kappa), \qquad \kappa = 1, 2 \ldots \beta$$

is a rational function of t for $S(R, x_1)$ and is furthermore a divisor of $F(t)$. Hence $F(t, 1, 0)$ has the β-tuple root $t = x_1$, and $\therefore$ $x_2, \ldots x_m$ are also β-tuple roots of $F(t, 1, 0)$. Hence $j \geqq m\beta$.

But we show also that $j \leqq m\beta$. For the product of degree $m\beta$ in t

$$H(t, u, v) = \Pi\, G(t, x_\iota), \qquad \iota = 1, 2, \ldots m,$$

has a rational divisor for R in common with $F(t, u, v)$. Hence F is a divisor of H; $\therefore$ $j \leqq m\beta$.

Thus $j = m\beta$. But in our reasoning on $F(t)$ we can interchange x and y and it still holds. This would interchange m, n also α, β. Hence $j = n\alpha$.

47. Some Immediate Consequences of Kronecker's Theorem.

THEOREM I. *Let m be the order of the body $R(\xi, \eta_1, \eta_2 \ldots)$. The order n of any of its inferior bodies is a divisor of m.*

For let η be used to generate $S(\eta, \eta_1, \eta_2 \ldots)$, an inferior body of R of order n; and let ξ and η satisfy respectively the irreducible equations

$f(x) = 0$, $g(y) = 0$. Since η is a rational function of ξ for $R(\eta_1, \eta_2 \ldots)$ the adjunction of ξ splits from g a rational linear factor. Applying Kronecker's theorem we have $m = n\alpha$, since here $\beta = 1$.

Definition. α is called the *relative degree* of $R(\xi)$ with respect to $S(\eta)$.

THEOREM II. *If the adjunction of a root y_1 of an irreducible equation $g(y) = 0$ of degree n reduces the group G of an equation $f(x) = 0$ to a subgroup of index i, then n is a multiple of i and hence never less than i.*

For let $F = 0$, of degree m, be the Galoisian resolvent of $f = 0$. After the adjunction let its degree be α. From Kronecker's theorem the adjunction of a root, V, of $F = 0$ must make $g(y)$ reducible and the degree β of the irreducible factor for which y_1 is a root satisfies $m\beta = n\alpha$. As $m/\alpha = i$, we have $n = i\beta$.

THEOREM III. *The letters having the same meaning as above, suppose $n = i$* [this is always so if n is a prime]. *Then $g(y) = 0$ is a rational resolvent.*

For here $\beta = 1$. Hence one root y_1 of $g(y) = 0$ is a rational function of $V = u_1 x_1 + u_2 x_2 + \ldots$, *i. e.* of the roots $x_1, x_2 \ldots$ of $f(x) = 0$; $\therefore$

$$y_1 = \phi(x_1, x_2, \ldots).$$

Apply the substitutions of G to ϕ: it goes over into say $\phi_1, \phi_2, \ldots$ The ϕ's are roots of an irreducible equation $\Phi = 0$. The two irreducible equations $g = 0$, $\Phi = 0$, having one root in common, are identical. Hence all the roots of $g = 0$ are rational in the x's.

THEOREM IV (JORDAN).* *The domain being R, let the adjunction of all the roots $y_1, y_2, \ldots$ of $g(y) = 0$ reduce the group G of the equation $f(x) = 0$ to a subgroup G_1, of index i; then the adjunction of all the roots $x_1, x_2, \ldots$ of $f = 0$ reduces the group H of $g = 0$ to a subgroup H_1 of index k. Furthermore $i = k$ and G_1, H_1 are invariant.*

1° $i = k$. Let the orders of G, H, G_1, H_1 be respectively g, h, g_1, h_1; and let $g = i\alpha$, $h = k\beta$. Then by Kronecker's theorem $g\beta = h\alpha$. For the adjunction of $x_1, x_2 \ldots$ is the same as adjoining one root of the Galoisian resolvent of $f = 0$; and the same applies to the y's and the equation $g = 0$. Multiplying the equation $g\beta = h\alpha$ through by i, we infer that $i\beta = h$, and hence $i = k$.

---

* First published *Math. Annalen*, vol. 1 (1869), p. 139. Kronecker's theorem was first published in a paper by Kneser, *Math. Annalen*, vol. 30 (1887), p. 195. We wish to remark that although we have made Jordan's theorem depend on Kronecker's, it is on the much older theorem of Jordan's that most of the following work directly rests.

2° G_1, H_1 *are invariant.* For the group of $f(x) = 0$ for $S(y_1\, y_2 \ldots)$ being G_1, let $\phi(x_1, x_2 \ldots)$ be a rational function for R of the x's, belonging to G_1. Then ϕ is rationally known for S, §12, 1°; *i. e.*

$$\phi = \psi(y_1, y_2, \ldots).$$

For the substitutions of G, ϕ considered as a function of the x's will take on certain values $\phi, \phi_1, \phi_2, \ldots$, which are roots of an irreducible equation $\Phi = 0$ for R. Considered as a function of the y's, $\phi = \psi$ takes on certain values $\psi, \psi_1, \psi_2, \ldots$ for the substitutions of H. These are roots of an irreducible equation $\Psi = 0$ for R. The two equations $\Phi = 0$, $\Psi = 0$, having a root $\phi = \psi$ in common, are identical. Hence the conjugate functions $\phi_1, \phi_2, \ldots$ are rational functions of $y_1, y_2, \ldots$ for R. Their adjunction cannot therefore reduce G below G_1. Hence G_1 is invariant. The same reasoning applies to H and H_1.

THEOREM V. *When the group H above is simple, $g(y) = 0$ is a rational resolvent for R.*

For the adjunction of the x's reduces H to some invariant subgroup. As it is simple, this subgroup is 1. But when the Galoisian group of an equation $g(y) = 0$ is 1 the roots of $g = 0$ must be rationally known.

THEOREM VI (GALOIS). *The necessary and sufficient condition for the algebraic solubility of an equation is that its group admits a series of composition whose factors are all primes.*

In §31 we showed this condition to be sufficient. Theorems III and IV of the present § will enable us to show that it is also necessary. Let us recall more precisely what we mean by saying an equation can be solved *algebraically*. We may say in general: to solve an equation $f = 0$ is to express rationally its roots in the roots of certain equations

$$f_1 = 0, \quad f_2 = 0, \quad f_3 = 0, \ldots, \tag{1}$$

which from a certain standpoint are simpler than $f = 0$. When the equations (1) are binomial equations

$$y^m - a = 0 \tag{2}$$

we say the solution is *algebraic*. In seeking, then, an algebraic solution of $f = 0$, we suppose the method of solving binomial equations already known. Since the various roots of (2) differ only by an mth root of unity, these are also known by implication, and we can suppose them to lie in our initial domain.

If, then, the given equation $f(x) = 0$ can be solved algebraically, some-

time on adjoining the roots of an equation of the type (2) the group of $f(x) = 0$ must suffer a reduction. The equations (2) can be simplified. Since the $r$sth root equals the rth root of the sth root we can suppose m is a prime. Furthermore we can suppose a is not the mth power of a quantity in the current domain R. For then the roots of (2) already lie in R. Under these circumstances (2) is irreducible for R, §45. As the adjunction of the roots of (2) reduces the group, they reduce it to an invariant subgroup, say of index i, by virtue of Theorem IV. As the adjunction of one root has the same effect as that of all, Theorem III shows that $i = m$, a prime.

From Theorem VI we conclude:

THEOREM VII (ABEL). *Whenever an equation $f(x) = 0$ can be solved algebraically, we can give the expressions for the roots such a form that all radicals $R_1, R_2, \ldots$ entering them are rational integral functions of the x's and certain roots of unity with coefficients which are integers. The radicals $R_1, R_2, \ldots$ form a sequence,*

$$R_1^{p_1} = F_1, \quad R_2^{p_2} = F_2, \ldots\ldots R_l^{p_l} = F_l, \tag{1}$$

where F_s is rational in the radicals $R_{s-1}, \ldots R_1$, and quantities in the original domain R. The exponents are primes and the equations (1) are irreducible in their current domains.

In fact such unit roots being adjoined as are necessary, let G be the group of $f = 0$. By the last theorem we saw it admits a series of composition

$$G, G_1, G_2, \ldots G_l = 1,$$

whose factors,

$$p_1, p_2, \cdots p_l,$$

are primes.

Let $\phi(x_1, x_2, \ldots)$ be an integral rational function of the roots of $f = 0$ belonging to G_1, and let it take on the values $\phi, \phi_1, \ldots \phi_{p_1-1}$ for G. Build now the cyclic function, §31,

$$\phi + a\phi_1 + \ldots + a^{p_1-1}\phi_{p_1-1} = R_1,$$

where a is an imaginary p_1th root of unity. Then R_1 is an integral rational function of the roots of $f = 0$ and certain roots of unity, whose p_1th power F_1 is rationally known. The adjunction of the roots of

$$R_1^{p_1} = F_1$$

reduces G to G_1. We proceed in the same way with the other radicals.

Some Celebrated Problems of the Past.

48. Statement of the Problems. The theory of *irrational* resolvents enabled us to deduce Galois' criterion for the algebraic solubility of an equation. This is one of Galois' most brilliant achievements. We turn now to the consideration of certain celebrated problems which have baffled the efforts of past mathematicians and show how by employing *irrational* resolvents they may be readily disposed of.

They are: 1° the Delian problem, or the duplication of the cube; 2° the construction of regular polygons; 3° the trisection of a given angle; 4° the *casus irreducibilis*; 5° the algebraic solution of the general equation of the fifth degree.

The Delian Problem is this: Being given the length of an edge of a cube, construct geometrically, *i. e.* by rule and compass, the length of the edges of a cube twice the volume of the first. A pretty legend is connected with this problem which is more than two thousand years old. A pest was raging at Athens. To obtain its abatement the Athenians sent to consult the oracle at Delphi. The reply came back that the plague would stop if the Athenians would dedicate to Apollo's temple at Delos an altar just double in size the one then there, which was a cube of gold. This the Athenians did, but the plague did not cease. They sent a second time to consult the oracle, which replied; the new altar was indeed double in *size* but they had neglected to make it an *exact cube*. The plague was sent, so it was thought, because the Athenians had neglected the study of geometry.

The problem is, then, to construct by rule and compass the real root of $x^3 - 2 = 0$.

The Construction of Regular Polygons was one of the favorite problems of Greek geometers. The construction by rule and compass of polygons of 3, 4, 5 and 15 sides and those immediately deducible from them by bisection was early found. The construction of other polygons baffled all their efforts. It was therefore a great surprise to mathematicians when Gauss showed (1801) that polygons of 17, 257, 65537 sides and in short all polygons the number of whose sides was a prime of the form $2^m + 1$* can also be constructed.

Let $\phi(n)$ denote as usual the number of integers $< n$ and relatively prime to n. We shall show that a polygon of n sides can then and only then be con-

* It remains to be seen whether $2^m + 1$ represents other primes than the five above given.

structed by rule and compass when $\phi(n)$ is a power of 2. The problem is thus brought to a definite close.

The Trisection of a Given Angle. This problem sprang from the preceding. For a polygon of 9 sides could be constructed if it were possible to trisect the arc subtended by the sides of the inscribed triangle. We shall generalize the problem and seek to divide *any* arc into n equal parts.

The casus irreducibilis. This problem arose in connection with the solution of the cubic. If we suppose this brought to the form

$$x^3 + px + q = 0, \tag{1}$$

its roots have the well-known form

$$x = \sqrt[3]{-\tfrac{1}{2}q + \sqrt{R}} + \sqrt[3]{-\tfrac{1}{2}q - \sqrt{R}} \tag{2}$$

where $$R = \tfrac{1}{4}q^2 + \tfrac{1}{27}p^3 = -\tfrac{1}{6}\Delta.$$

Now when the roots of (1) are all real, the coefficients being real, the discriminant Δ is positive, and $\sqrt{R}$ is imaginary. (2) expresses thus the roots as the sum of two conjugate imaginary quantities. To Cardan and his contemporaries who had no idea how such cube roots could be found this case was highly paradoxical. Since that time mathematicians have attempted to present these real roots as sums of real radicals. As their efforts were unsuccessful, the case when $\Delta > 0$ was known as the *casus irreducibilis*. We show that this case is indeed irreducible.

The Algebraic Solution of the Quintic is another impossible problem which has engaged the attention of mathematicians for centuries. The impenetrable mystery which surrounded this problem was at length dispelled by Abel (1826). He showed that the roots of the *general* equation of the fifth and higher degrees cannot be expressed by means of radicals.

Abel's demonstration is very long and very abstruse; it was totally incomprehensible to the ordinary mathematician of his time and only imperfectly grasped by the best. Galois' theory affords us a very elegant and simple demonstration. We have in fact only to apply Galois' criterion §§ 31, 47.

49. Analytic Criterion for Geometric Constructions. The first three of these five problems depend upon the possibility or impossibility of constructing certain lines by rule and compass. To employ the reasoning of analysis we must deduce an analytic criterion for the possibility of these constructions. To this end we remark that each right line and circle employed in

the construction is represented analytically by an equation of first or second degree. All points determined by their intersection are thus defined by a sequence of irreducible equations of second degree with real coefficients

$$f_1 = 0, \quad f_2 = 0, \quad f_3 = 0 \ldots . \qquad (S)$$

The coefficients of the first equation lie in a domain R generated by numbers determined by the data of the problem. The coefficients of the succeeding equations lie in a domain formed by R and the roots of the preceding equations. This condition is necessary; that it is sufficient, follows from the fact that the square root of any real positive number can be constructed geometrically. Hence the

THEOREM. *The necessary and sufficient condition that a geometric construction can be effected by rule and compass is, that the coordinates of all points involved lie in a domain* Σ *generated by the roots of a sequence of the type* S.

COROLLARY. *A root* ξ, *real or complex, of an equation* $f(x) = 0$ *can be plotted by rule and compass in the complex plane when and only when* ξ *lies in a domain of the type* Σ. *The coefficients of* S *can be imaginary.*

50. The Delian Problem If the problem be possible, the real root of

$$x^3 - 2 = 0 \qquad (1)$$

must lie in a Σ-domain; the original domain R being here $R(1)$. Observe first that (1) is irreducible, §45. We prove now the

THEOREM. *If a root of an irreducible equation* $F(x) = 0$ *lie in a* Σ*-domain, its degree* m *is a power of* 2.

For then at some point, say on adjoining the roots of $f_\kappa = 0$, $F = 0$ becomes reducible. Kronecker's theorem requires that $m = 2a$, *i. e.* that $F = 0$ splits into two factors of equal degree. Since ultimately $F(x)$ must possess a rational linear factor, m can contain no factor other than 2.

The impossibility of the Delian problem now follows immediately.

COROLLARY. *In order that a root* ξ, *real or imaginary, of an irreducible equation* $f(x) = 0$ *can be constructed geometrically, it is necessary that the degree of* f *be a power of two.*

51. Construction of Regular Polygons. We seek all regular polygons which can be constructed by rule and compass. We reduce the problem to a simpler one. Evidently if a polygon of m sides cannot be constructed, one of mn cannot. Again if polygons of m and n sides can be

constructed, m and n being relatively prime, one of mn sides can be. For we can determine a, b so that $am + bn = 1$ whence $a/n + b/m = 1/mn$: *i. e.* b arcs of the first polygon plus a arcs of the second give an arc of a polygon of mn sides. Since every integer n can be decomposed in one way only into relatively prime factors

$$n = p^a q^b r^c \ldots \quad ; \qquad p, q, \ldots \text{ primes},$$

our problem is reduced to that of constructing a polygon, the number of whose sides m is a power of an odd prime $m = p^a$.

Consider such a polygon. Its vertices are the m points in the complex plane $1, \rho, \rho^2, \ldots$ roots of the equation $x^m = 1$. In the next § where we shall study this equation we shall see that its roots can be constructed by rule and compass when and only when $\phi(m) = p^{a-1}(p-1)$ is a power of two. As $\phi(mn) = \phi(m)\phi(n)$ we have the following elegant

THEOREM (GAUSS). *The necessary and sufficient condition that a polygon of n sides can be constructed by rule and compass is that $\phi(n)$ be a power of 2.*

52. The Roots of Unity. We recall first a few facts from elementary algebra.

If a and b are relatively prime the roots of the equations

$$x^a = 1, \quad x^b = 1 \tag{1}$$

have only unity in common. Hence if α be a root of the first and β a root of the second equation, $\alpha\beta$ is a root of $x^{ab} = 1$; furthermore all the roots of this last equation are got by letting α, β run over all the roots of their respective equations. Hence the solution of $x^n = 1$ depends upon the equations

$$x^{p^a} = 1, \qquad x^{q^b} = 1, \qquad \ldots . \tag{2}$$

where $p^a, q^b, \ldots$ are the relatively prime factors of n.

These equations are of the type

$$x^m = 1, \qquad (p^a = m) \tag{3}$$

There are two ways of treating this equation. The first is to set $x^p = y$, $y^p = z, \ldots . w^p = 1$, which reduces the solution of (3) to that of $a - 1$ binomial equations and the determination of the pth roots of unity.

The second way is to consider (3) directly. We prefer this latter method here. We assume p is odd; the case when p is even requiring only the extraction of square roots.

We begin by observing that (3) is not irreducible since evidently

$$x^m - 1 = (x^{p^{\alpha'}} - 1)(x^{(p-1)p^{\alpha-1}} + x^{(p-2)p^{\alpha-1}} + \cdots + x^{p^{\alpha-1}} + 1)$$

The second factor, call it $H(x)$, vanishes evidently for all and only for the primitive mth roots of unity. The solution of $H = 0$ and (3) are equivalent problems.

$H(x)$ is irreducible for $R(1)$. For let $H(x) = P(x)\,Q(x)$. The coefficients of P and Q are integers § 42, IV. Observe that $H(1) = p$ since $H(x)$ contains p terms. As this is a prime one of the factors $P(1)$, $Q(1)$ is ± 1; say $P(1) = \pm 1$. Consider now the product

$$\Phi(x) = \prod_{\lambda} P(x^\lambda)$$

where λ runs over all numbers $< m$ and not divisible by p. Then $\Phi(1) = \pm 1$.

Since $P(x)$ vanishes for one primitive mth root, $\Phi(x)$ vanishes for every primitive root $\therefore$ Φ is divisible by $H(x)$; say $\Phi(x) = H(x)\,K(x)$, $\therefore$ $\Phi(1) = H(1)\,K(1)$ or $\pm 1 = p \cdot K(1)$ which is impossible as $K(1)$ is an integer.

The group of $H(x) = 0$ for $R(1)$ is now easily obtained. The equation $H(x) = 0$ is irreducible and all its roots are rational functions of one of them. For such equations there exists the following

THEOREM. *Let $f(x) = 0$ be an irreducible equation of degree n and let all its roots be rational functions of one of them, say x_1. Then the order of its group G is n.*

For let $V_1 = u_1 x_1 + \cdots + u_n x_n$ be a root of the Galoisian resolvent. Consider the two bodies $R(V_1)$ and $S(x_1)$. As x_1 is a rational function of V_1, S is an inferior body of R. As all the roots of $f = 0$ are rational in x_1, V_1 is rational in x_1, $\therefore$ R is an inferior body of S, $\therefore$ $R = S$ and the degree of the Galoisian resolvent and hence the order of the group is n.

We can now determine the group Γ of $H = 0$. Let g be a primitive congruence root for the modulus m. Then $1, g, g^2 \ldots g^{\mu-1}$ (where $\mu = \phi(m)$) are incongruent, modulo m, and $x_\kappa = \rho^{g^\kappa}$ ($\kappa = 0, 1, \ldots \mu - 1$, $\rho = e^{\frac{2\pi i}{m}}$) are the roots of $H = 0$. Since $H = 0$ is irreducible, Γ is transitive and contains a substitution s which replaces x_0 by x_1 *i. e.* ρ by ρ^g. This substitution thus replaces x_κ by $x_{\kappa+1}$; $\therefore$ $s = (0, 1, 2, \ldots \mu - 1)$: $\therefore$ Γ contains also

$$1, s, s^2 \ldots s^{\mu-1} \qquad (a)$$

It can contain no more substitutions since the order of Γ is μ. We have thus the

THEOREM. *The group of $H(x) = 0$ for $R(1)$ consists of the μ substitutions (a).*

We prove now easily the

THEOREM. *The equation $H = 0$ is algebraically soluble supposing known the roots of unity whose indices are the prime factors of $\mu = \phi(m)$. The necessary and sufficient condition that its roots lie in a Σ-domain is that μ is a power of 2.*

For let q be any prime factor of $\mu = qr$. The r substitutions

$$1,\ t = s^q,\ t^2,\ \ldots\ t^{r-1}$$

obviously form an invariant subgroup Δ of Γ of index q. Hence the factors of composition of Γ are primes. Then §31 shows that Γ is reduced to Δ on extracting a qth root; we need however a qth root of unity.

Thus the calculation of the nth roots of unity is made to depend on the roots of unity of lower index. Evidently the preceding proves the

THEOREM. *The roots of unity may be found by extracting roots of known quantities.*

53. The Multisection of an Arbitrary Angle α. The division of α into n parts will be possible or not according as the roots of

$$x^n = a \tag{1}$$

lie in a Σ-domain where $a = \cos\alpha + i\sin\alpha$. As a will not in general be the nth power of a fraction, (1) is in general irreducible. Hence by §50 *Cor.* we have the

THEOREM. *Any division of an angle, besides bisection, is in general impossible, making use only of rule and compass.*

54. Casus Irreducibilis. That the attempt to express the roots of the cubic for this case by real radicals is impossible and that this *casus* is indeed *irreducibilis* is made manifest by the following general

THEOREM. *An irreducible equation $f(x) = 0$ of degree n whose roots are all real can never be solved by real radicals alone if n contains other factors than 2.*

For proceed to adjoin real radicals of prime index. Suppose the first reduction of the group G takes place on adjoining a root of

$$y^p - a = 0. \tag{1}$$

Here a by hypothesis is real. It cannot be the pth power of a quantity in the

current domain R, for then the adjunction of the real root could not reduce G. Hence (1) is irreducible for R. Hence by Theorem III, §47, all the roots of (1) are rational functions of the roots of $f = 0$, therefore they are real, which is absurd, if $p > 2$.

55. Impossibility of Solving Algebraically the General Equation of Degree $n > 4$; Hilbert's Investigations. Of the five problems we selected to illustrate the use of irrational resolvents, this is at once the most celebrated and difficult. We saw §15 that the group of the general equation $f(x) = 0$ of degree n for a domain R, containing the coefficients which are variables, and such constants as we choose, is the symmetric group S_n. To see if $f = 0$ is algebraically soluble for R we have simply to investigate the factors of composition of S_n. For $n = 2, 3, 4$ we saw these were primes. For $n > 4$ they are not primes. We show, in fact, that the only invariant subgroup of S_n besides 1 is a subgroup of index 2. This group is called the *alternate* group. The *only* factors of composition of S_n are thus 2, $\frac{1}{2}n!$. The latter not being a prime we have the

THEOREM (RUFFINI, ABEL). *The general equation of degree $n > 4$ cannot be solved algebraically.*

The demonstration that the factors of composition of S_n are not primes is rather lengthy. A much shorter demonstration of the Ruffini-Abelian Theorem can be given by making use of Abel's theorem of §47. We prefer to give here a demonstration which rests on the factors of composition of S_n because, in the first place, it establishes the theorem in question by a general principle, viz. the criterion of Galois, and secondly because to do this we shall need to develop a little more the theory of substitution groups which has been rather meagerly treated in this paper. Before going on we must call attention to a remarkable paper by Hilbert, *Crelle*, vol. 110, pp. 104–129. The theorem of Ruffini-Abel is unsatisfying as it stands; it asserts indeed that the general equation of degree >4 is unsolvable by radicals, but it says nothing about special equations. It might well happen, as Dirichlet remarked, that every equation with integral coefficients was algebraically soluble. This is due to the fact that an integral rational function $G(t_1, t_2 \ldots; u_1, u_2 \ldots)$ of certain variables $t_1, t_2 \ldots$ and indeterminates $u_1, u_2 \ldots$ may well be irreducible for $R(1)$ as long as the u's were left indeterminate and yet be reducible for all integral sets of the u's. That this is not so, that in fact we can give the u's integral values $b_1, b_2 \ldots$ in an infinite variety of ways so that $G(t_1, t_2 \ldots; b_1, b_2 \ldots)$ is irreducible was shown by Hilbert in the paper just mentioned.

From this follows at once that there is an infinite number of equations with integral coefficients whose group for $R(1)$ is the symmetric group. From this we conclude immediately that there is an infinity of equations with integral coefficients whose group for $R(1)$ is any prescribed group.

Excursus on Substitution Groups.

56. Odd and Even Substitutions. *Definition.* A *transposition* is a cycle of order 2.

Thus $(1, 2), (a, b)$ are transpositions. *Every substitution can be represented as a product of transpositions.* For we showed §6 that every substitution could be represented as a product of cycles. Evidently every cycle can be expressed as a product of transpositions.

Thus $$(1\ 2\ 3\ 4\ 5) = (12)\,(13)\,(14)\,(15).$$

We can represent a substitution as a product of transpositions in an infinite number of ways. Another decomposition of $(1\ 2\ 3\ 4\ 5)$ into transpositions would be, *e. g.*,

$$(1\ 2\ 3\ 4\ 5) = (13)\,(24)\,(23)\,(34)\,(14)\,(15).$$

We observe however the

Theorem: *The number of transpositions into which a substitution can be decomposed is always odd or always even.*

In fact let $S = ABC\ldots L$ be a substitution of s elements consisting of γ cycles $A, B, \ldots$ Let t be a transposition. Then St contains one more or one less cycle than S.

For the two letters of t are 1° either in the same cycle, A, or 2° in different cycles, A, B.

1° Let $A = (a_1 \ldots a_m), \qquad t = (a_1 a_r)$;

then $St = (a_1 \ldots a_{r-1})(a_r \ldots a_m)B \ldots L$, which has one cycle more than S.

2° Let $A = (a_1 \ldots a_m), \quad B = (b_1 \ldots b_n), \quad t = (a_\alpha b_\beta)$; then $St = (a_1 \ldots a_{\alpha-1}\, b_\beta \ldots b_n\, b_1 \ldots b_{\beta-1}\, a_\alpha \ldots a_n)C \ldots L$, which has one cycle less than S.

This established, let $t_1, t_2 \ldots$ be transpositions. Then St_1 has $\gamma + 1$ or $\gamma - 1$ cycles. $St_1 t_2$ has $\gamma + 2$, γ or $\gamma - 2$ cycles. In general $St_1 \ldots t_\tau$ has $\gamma - T$ cycles, where T is odd or even with τ.

Multiply now S by $(t_1 \ldots t_\tau)^{-1} = t_\tau \ldots t_1$; we have

$$A B \ldots L t_\tau \ldots t_1 = 1. \qquad (1)$$

As the identical substitution is the product of s cycles each containing only one element of S, the left side of (1) contains n cycles. $\therefore\ n = \gamma - T$, $\therefore\ T$ and hence also τ is odd or even with $n - \gamma$ which is invariant.

This theorem affords us a means of classifying substitutions.

Definition. A substitution is said to be *odd* or *even* according as the number of transpositions which represent it is odd or even.

57. The Alternate Group A_n. Since the product of two even substitutions is even, the even substitutions of any group form a subgroup.

Definition. The group formed by the even substitutions of the symmetric group S_n is called the alternate group, A_n.

THEOREM I. *The order of A_n is $\frac{1}{2}\,n!$* In fact the even substitutions of any group G form a subgroup of index 2. For let

$$g_1,\ g_2,\ g_3 \ldots$$

be the even substitutions of G, and let ω be any odd substitution of G.

$$\omega g_1,\ \omega g_2,\ \omega g_3 \ldots$$

are evidently odd; they are also distinct. Hence there are at least as many odd as even substitutions. Let now the g's represent the odd substitutions of G and ω an even substitution. The same reasoning shows there are at least as many even as odd substitutions.

THEOREM II. *A_n is an invariant subgroup of S_n.* For let a be any substitution of A_n and s any substitution of S_n. Then a is even by definition. Also s^{-1} is odd or even with s. For if $s = t_1 \ldots t_\tau$ be a representation of s by transpositions, $s^{-1} = t_\tau \ldots t_1$. Hence $s^{-1} a s$ is even, and so lies in A_n.

THEOREM III. *If a group contains* 1° *all cyclic substitutions of the third order or* 2° *even the cyclic substitutions*

$$(1\,2\,3),\quad (1\,2\,4),\ \ldots\ (1\,2\,n) \qquad (a)$$

it contains A_n.

1° For the substitutions of A_n are products of *pairs* of transpositions. These pairs are either of the type $(a\,b)\,(c\,d)$ or $(a\,b)(a\,c)$.

But
$$(a\,b)(c\,d) = (a\,b\,c)(c\,a\,d)$$
$$(a\,b)(a\,c) = (a\,b\,c)$$

Hence A_n contains no substitution which is not the product of cyclic substitutions of the third order.

2° Every pair of transpositions can be represented as a product of the substitutions (a). For any transposition $(a\,b)$ can be written $(1\,a)\ (1\,b)(1\,a)$. Hence every substitution in A_n is the product of pairs of the transpositions,

$$(11),\ (12),\ (13),\ \ldots\ (1n).$$

But any such pair can be written

$$(1\,a)\ (1\,b) = (12\,a)(12\,a)(12\,b).$$

58. Series of Composition of S_n. We have just seen that A_n is an invariant subgroup of S_n. It is maximum since its index is 2, the smallest possible. We prove now the

THEOREM. *The only series of composition of S_n is*

$$S_n,\ A_n,\ 1\ ; \qquad n > 4.$$

We show 1° A_n is simple; 2°, S_n contains no other invariant groups.

1° *A_n is simple.* For let B be an invariant subgroup different from 1. Let a, b be substitutions of A_n and B respectively. Then $\beta = b^{-1}a^{-1}ba$ lies in B since b^{-1} and $a^{-1}ba$ do. The operation which converts b into β call T. By the aid of these T transformations we show B must contain at least one cyclic substitution of order 3. Begin by observing that every substitution in S_n has one of the following 7 forms when written as a product of cycles, §6. The letters C_1, C_2 . . . represent cycles whose orders call c_1, c_2 . . . respectively.

I;	$(12\ldots m)\,C_1\,C_2\ldots$	$m \geqq 4$
II;	$(1\,2\,3)\,(4\,5\,6)\,C_1\,C_2\ldots$	$c_1, c_2, \ldots \leqq 3$
III;	$(1\,2\,3)\,(4\,5)\,C_1\,C_2\ldots$	$c_1, c_2, \ldots \leqq 2$
IV;	$(1\,2)\,(3\,4)\,(5\,6)\,C_1\,C_2\ldots$	$c_1, c_2, \ldots \leqq 2$
V;	$(1\,2)\,(3\,4)\,C_1, C_2\ldots$	$c_1, c_2, \ldots = 1$
VI;	$(1\,2)\,C_1\,C_2\ldots$	$c_1, c_2, \ldots = 1$
VII;	$(1)\,(2)\,(3)\ldots(n)$	

Type VI cannot occur in B since this contains only even substitutions. Consider now a substitution of B other than the identical substitution. It it be of κth type denote it by b_κ, $\kappa = 1, 2, 3, 4, 5$. Transform b_κ by T_κ which is got by using a_κ where $a_1 = (123)$, $a_2 = (145)$, $a_3 = (124)$, $a_4 = (135)$, $a_5 = (135)$. As a result we get β_κ where $\beta_\kappa = b_\kappa^{-1}a_\kappa^{-1}b_\kappa a_\kappa$. Then $\beta_1 = (124)$, $\beta_2 = (14526)$, $\beta_3 = (12534)$, $\beta_4 = (135)(264)$, $\beta_5 = (13542)$. Hence if B contains a substitution of type I, T_1 converts it into a cyclic substitution of order 3. If B contains a substitution of type II, T_2 converts it into one of

type I, etc. Hence B contains a cyclic substitution of order 3; let it be $b = (123)$. Let $a = (1\,r\,3)$; then $c = a^{-1}ba = (r\,21)$ and $\therefore c^2 = (12\,r)$ are in B, $r = 4, 5, \ldots n$. Hence $B = A_n$. §57 Theorem III.

2° *S_n contains no other invariant groups.* For let C be such a group. If C contain substitutions of the types I—V it contains A_n. It can thus contain only substitutions of types VI, VII, *i. e.* besides 1, only transpositions. It can contain but one transposition t, for otherwise it would contain an even substitution $\neq 1$. Hence $C = \{1, t\}$. On suitably choosing a substitution s in S_n, $s^{-1}ts$ is any transposition at will $\therefore C = S_n$.

The Essential Elements of any Solution of an Equation.

59. Abstract Groups. To solve an equation $f(x) = 0$ means to express its roots rationally in the roots of certain equations

$$f_1 = 0, \qquad f_2 = 0 \ldots . \tag{1}$$

whose roots we suppose can be found or whose properties we suppose to be sufficiently studied. Since the resolvents (1) can be varied infinitely, the question arises: what remains invariant for these changes?

We proceed to show that the group G of $f = 0$ determines certain groups

$$\Gamma_1, \ \Gamma_2, \ldots ., \tag{2}$$

and that the sequence (1) must contain equations whose groups are the groups (2). If the solution is conducted as expeditiously as possible, the sequence (1) need contain only these last equations. These then are essential elements in every solution of the given equation.

This statement we must explain in detail; we begin by generalizing our notion of a group, which up to the present has been restricted to substitution groups.

Definition. Suppose a finite number of things or elements $T_1, T_2, \ldots T_n$ given; we say they form a group if

(a) A law of composition is given whereby from T_a and T_b, taken in a definite order, a definite T_c is determined. The composition we call multiplication, and write $T_a\,T_b = T_c$.

(b) Multiplication is associative, although not necessarily commutative.

(c) There exists one and only one element T_1, for which

$$T_1\,T_\kappa = T_\kappa\,T_1 = T_\kappa \qquad \kappa = 1, 2, \ldots n$$

This element is called the *identical element* and is conveniently represented by 1.

(d) For every element T_κ exists an element (denote it by T_κ^{-1}) such that

$$T_\kappa T_\kappa^{-1} = T_\kappa^{-1} T_\kappa = 1.$$

T_κ^{-1} is called the *inverse* of T_κ.

Examples: 1° *Substitution Groups.* That the elements of such groups have the properties (a) to (d) is obvious. Conversely, every finite group that satisfies the above conditions is isomorphic with a substitution group.

2° *Groups of Rotations of the Regular Bodies.* The rotations which bring one of the regular bodies into coincidence with itself have obviously the properties (a) to (d).

Consider, for example, the tetrahedron whose vertices call V_0, V_1, V_2, V_3. Let A be a rotation of 120° about the perpendicular from V_0 on the opposite face. Let S be a rotation about the diagonal joining the middle point of $V_0 V_1$ and the corresponding point of the opposite edge; similarly let T be a rotation about the corresponding diagonal determined by $V_0 V_2$. All possible positions of the tetrahedron are produced by the 12 rotations

$$A^a S^b T^c, \qquad a = 0, 1, 2; \qquad b, c = 0, 1.$$

These obviously form a group in the above sense.

3°. *Congruence Groups.* Let p be a prime; we throw all integers not divisible by p into $p-1$ classes so that all integers congruent to each other, mod p, fall into one class, while incongruent numbers belong to different classes. Thus:

C_1; $\quad 1, \quad p+1, \quad 2p+1, \quad 3p+1, \ldots.$
C_2; $\quad 2, \quad p+2, \quad 2p+2, \quad 3p+2, \ldots.$

. . . . . .

C_{p-1}; $\quad p-1, \quad 2p-1, \quad 3p-1, \quad 4p-1 \ldots.$

We define the multiplication of these classes thus: $C_a C_b = C_c$ where c is the smallest positive residue of ab, mod p. We can show at once that the C's form a group.

Definition. All terms used in substitution groups, as *subgroups*, *invariant subgroups*, *order*, *index*, *isomorphism*, etc., we extend to all these groups, which we call *abstract groups*.

Two abstract groups G, H which are 1–1 isomorphic are evidently, as

far as structure goes, not distinct. From this abstract standpoint we shall consider them as identical and write $G = H$.

60. Factor Groups. Referring to §28 we observe that an invariant subgroup $I(1, a, b, \ldots)$ of a group $G(g_1 = 1, g_2, \ldots)$ can be used to define another abstract group. In fact, as the table B shows, I may be used to divide G into ρ classes $C_1, C_2 \ldots C_\rho$, the substitutions of each row constituting a class. To define the multiplication of the C's let us designate the substitutions* $\alpha, \beta, \ldots$ of J by new symbols $j_1 = 1, j_2, \ldots j_\rho$, which are more convenient for our present use. Let us in fact designate by j_κ the substitution of J which corresponds to the substitutions of G in the κth row of B, *i. e.* the substitutions which form C_κ. We define now $C_\iota C_\kappa$ to be C_λ where λ is the index in $j_\iota j_\kappa = j_\lambda$. Obviously the classes $C_1, C_2, \ldots$ form a group which is 1–1 isomorphic to J.

Definition. The group $C_1, C_2, \ldots C_\rho$ is called a *factor group* and is written G/I. Observe then that $G/I = J$.

We can evidently generalize this. Let G be, instead of a substitution group, any abstract group. By means of its invariant subgroups I, we can form a perfectly analogous table to B, which as before may be used to throw the elements of G into a certain number of classes $C_1, C_2, \ldots$ Take now *any* element, say ag_ι in C_ι and *any* element, say bg_κ, in C_κ. The product $ag_\iota \cdot bg_\kappa$ always lies in one and the same class, say C_λ, however a, b be chosen, *i. e.*, λ depends only on ι, κ. We define then multiplication just as before and set $C_\iota C_\kappa = C_\lambda$ where λ is determined as just stated. The C's form a group as before which we also call a factor group of G, and write G/I.

We develop now some theorems on factor groups. As the reasoning is the same we suppose our groups are any abstract groups. The first eight theorems lead up to Theorems IX and X which are the ones we need.

THEOREM I. *Let* $H(h_1 = 1, h_2 \ldots)$, $K(k_1 = 1, k_2 \ldots)$ *be any two invariant subgroups of* G $(g_1 = 1, g_2 \ldots)$; *the elements common to* H *and* K *form an invariant subgroup* $C(c_1 = 1, c_2, \ldots)$ *of* G.

For $g^{-1}cg$ lies in H, if we consider c to be in H, and in K, if we consider c to be in K; $\therefore$ it lies in both H and K and hence in C.

THEOREM II. *G, H, K, C being as before, let*

$G/C = \Gamma(\gamma_1 = 1, \gamma_2 \ldots)$, $H/C = \Delta(\delta_1 = 1, \delta_2 \ldots)$, $K/C = \Theta(\theta_1 = 1, \theta_2 \ldots)$; *then Δ and Θ are invariant subgroups of Γ.*

---

* For the notation *cf.* § 28.

Consider, for example, Δ; the same reasoning applies to Θ. We arrange our groups in the following array. Similar arrays should be written down by the reader in the succeeding theorems.

	G	Γ	
H	$c_1=1,\ c_2,\ c_3,\ \ldots$	$\gamma_1=1$	Δ
	$h_2,\ c_2h_2,\ c_3h_2\ \ldots$	γ_2	
	$h_3,\ c_2h_3,\ c_3h_3\ \ldots$	γ_3	
	. . . . .	.	
	. . . . .	.	
	. . . . .	.	
	. . . . .	.	

We observe that the elements of G corresponding to $\gamma^{-1}\delta\gamma$ have the form $g^1\, ch\, g$ and this is an element of H, since it $= g^{-1}cg\cdot g^{-1}hg = c'h' = h''$; $\therefore$ $\gamma^{-1}\delta\gamma$ is an element of Δ.

THEOREM III. *Assuming here and in the following theorems that H and K are maximum; then Δ, Θ have only 1 in common.*

For to an element common to Δ and Θ correspond elements of G common to H and K, *i. e.*, elements of C. But to C corresponds only 1 in Γ.

Definition. When the elements of one group are commutative with all the elements of another group the two groups are called *commutative.*

THEOREM IV. *The groups Δ, Θ are commutative.*

$$\text{For } \sigma = \delta^{-1}\theta^{-1}\delta\theta = \delta^{-1}\cdot\theta^{-1}\delta\theta = \delta^{-1}\delta' = \delta''$$
$$= \delta^{-1}\theta^{-1}\delta\cdot\theta = \theta'\theta = \theta''.$$

Hence σ lies in Δ and Θ; $\therefore$ $\sigma = 1$ and $\delta\theta = \theta\delta$.

Definition. The group A which is formed by multiplying all the elements of two commutative groups B, C is called the *product* of B and C and is written $A = BC = CB$.

THEOREM V. *The group $\Omega = \Delta\Theta$ is identical with Γ.*

Observe first that Ω is invariant under Γ, since

$$\gamma^{-1}\omega\gamma = \gamma^{-1}\cdot\delta\theta\cdot\gamma = \gamma^{-1}\delta\gamma\cdot\gamma^{-1}\theta\gamma = \delta'\theta' = \omega'.$$

Hence the group O in G corresponding to Ω is invariant under G. But O containing H and K must be G.

THEOREM VI. $\Gamma/\Delta = \Theta$ *and* $\Gamma/\Theta = \Delta$.

Consider Γ/Δ; the same reasoning applies to Γ/Θ.

From Theorem V we can arrange Γ in the array

$$(b) \qquad \begin{array}{llll} \delta_1 = 1, & \delta_2, & \delta_3, & \ldots \\ \theta_2, & \delta_2\theta_2, & \delta_3\theta_2, & \ldots \\ \cdot & \cdot & \cdot & \cdot \end{array}$$

But from (b) we conclude at once $\Gamma/\Delta = \Theta$.

THEOREM VII. $G/H = K/C$ *and* $G/K = H/C$.

Consider G/H; the same reasoning applies to G/K. We throw G into the array

$$(\beta) \qquad \begin{array}{llll} h_1 = 1, & h_2, & h_3, & \ldots \\ g_2, & h_2 g_2, & h_3 g_2, & \ldots \\ \cdot & \cdot & \cdot & \cdot \end{array}$$

This defines a factor group G/H. If now we replace $\delta_1, \delta_2 \ldots$ in (b) by the elements of G we get exactly the first row in (β). That is, (b) and (β) define the same factor group Θ; $\therefore$ $G/H = \Gamma/\Delta = \Theta$.

THEOREM VIII. *C is a maximum invariant group under H and K.*

For since $H/C = G/K$, if C were not maximum under H, K would not be maximum under G.

THEOREM IX. *Let*

$$(1) \qquad G,\ G_1,\ G_2,\ \ldots\ 1$$
$$(2) \qquad G,\ H_1,\ H_2,\ \ldots\ 1$$

be two series of composition. The factor groups

$$G/G_1,\ G_1/G_2,\ \ldots\ldots$$
$$G/H_1,\ H_1/H_2,\ \ldots\ldots$$

are, aside from their order, identical. They are an invariant of the group G.

We prove this by induction, showing that if it is true for groups of order m it is true for those of order $\leqq 2m$. For $m = 2$ it is obviously true. Let then C be the group of elements common to G_1, H_1. By Theorem VIII, C is maximum under G_1 and H_1 and the factor groups of

$$(3) \qquad G,\ G_1,\ C,\ \ldots\ 1$$
$$(4) \qquad G,\ H_1,\ C,\ \ldots\ 1$$

are by Theorem VII identical. But, by the hypothesis for induction, the factor groups of

$$G_1,\ G_2,\ \ldots\ 1$$
$$G_1,\ C,\ \ldots\ 1$$

are identical. Hence the factor groups of (1), (3) are identical. Similarly those of (2), (4) are; ∴ those of (1), (2) are identical.

From Theorem IX follows as corollary

THEOREM X. *The factors of composition of any group are invariant.*

61. Hölder's Theorem. We are ready now to formulate precisely the statements made at the beginning of §59. This gives us

HÖLDER'S THEOREM: *For a domain R_0 let $f = 0$ have the group G whose factor groups, say, are $F_1, F_2, \ldots F_m$. Let the roots $x_1, x_2, \ldots x_n$ of $f = 0$ be rational in one or more roots of each of the equations*

$$(A) \qquad h_0 = 0, \quad h_1 = 0, \ldots h_{r-1} = 0.$$

Here the coefficients of h_ι lie in a domain R_ι which in turn lies in a domain generated by R_0 and all the roots of $h_0, h_1, \ldots h_{\iota-1}$. Let the group of $h_\iota = 0$ for R_ι be H_ι. Then the F's must be contained among the factor groups — call them $\Phi_1, \Phi_2 \ldots$ — of the H's. If the Φ's contain only the F's, the equations A are rational resolvents for R_0. If we suppose the equations A to be simple, $r \geqq m$. If $r = m$ and the equations A are simple, then these equations are rational resolvents for R_0.

In fact, begin by replacing A by simple equations, §29. We get the sequence

$$(B) \qquad k_0 = 0, \quad k_1 = 0, \ldots . \; k_s = 0,$$

whose groups K_ι for their respective domains S_ι must be the Φ's.

Consider the two equations $k_1 = 0$ and $k_\iota = 0$ for the common domain S_ι. If the adjunction of the roots of $k_1 = 0$ reduce K_ι, the roots of $k_\iota = 0$ are rational in those of $k_1 = 0$ by §47, V, and $k_\iota = 0$ can be dropped from B. Let

$$(B') \qquad k_0 = 0, \quad k_1' = 0, \quad k_2' = 0 \ldots .$$

be the sequence obtained by dropping out all such k_ι's. Here we can reason with $k_1' = 0$ just as we did with $k_1 = 0$. We shall thus drop out of B' all k's whose groups are reduced on adjoining the roots of $k_1' = 0$. The resulting sequence we treat in the same way. Finally we arrive at a sequence:

$$(C) \qquad k_0 = k_{a_0} = 0, \quad k_{a_1} = 0, \ldots . \; k_{a_{r-1}} = 0.$$

Here the domain of $k_{a_\iota} = 0$ is generated by R_0 and all the roots of the preceding equations in C. For this domain, let its group be T_ι. The T's lie among the K's.

Adjoin now to $f = 0$ the roots of $k_0 = 0$; if a reduction of G takes place let the new group be Γ_0. Then by §47, V, $k_0 = 0$ is a rational resolvent and by §60, $T_0 = G/\Gamma_0$. Adjoin now the roots of $k_{a_1} = 0$. If a reduction of Γ_0 takes place let the new group be Γ_1. Then $k_{a_1} = 0$ is a rational resolvent and $T_1 = \Gamma_0/\Gamma_1$. On adjoining the roots of the last equation of C the group of $f = 0$ is 1. Hence the Φ's embrace all the F's. If the Φ's embrace only the F's, the sequence C must be identical with B, and we can adjoin the roots of no equation of B without a reduction of the group of $f = 0$. Hence all the equations B and hence all the equations A are rational resolvents for R_0. Hence in every case $r \geqq m$.

If we suppose the equations A to be simple and $r = m$, then $A = B = C$ and the equations A are rational resolvents for R_0.

Every quantity not lying in a domain of rationality D may be called an *irrationality* with respect to D. If it is root of a rational resolvent we call it a *natural* irrationality, otherwise an *accessory* irrationality, in so far as it is used in the solution of the given equation.

62. The General Quintic $Q = 0$. Hölder's theorem is one of the most important and fundamental contributions to Galois' theory in recent years. Speaking roughly, it asserts that however the solution of a given equation $f(x) = 0$ be conducted, sometime in the course of the solution certain simple equations whose groups are uniquely determined and known in advance must be employed.

When $f(x) = 0$ is itself simple it can be solved by no simple equation $g(y) = 0$ essentially different from $f = 0$. In fact §47, V, shows that the y's are rational in the x's and conversely.

But of all simple equations $f = 0$, $g = 0$, . . . having a certain group there will be some whose properties will recommend them as *normal* equations. The reduction of $f = 0$, $g = 0$, . . . to such normal equations is a problem by itself.

We illustrate the use of normal equations on the quintic $Q = 0$. On adjoining the square root of its discriminant its group is A_5, which is simple. Other algebraic equations having this group arise in the theory of linear differential equations and the elliptic functions. The roots of these latter equations we can express in terms of the hypergeometric function or elliptic modular functions; besides they have many other elegant properties, which recommend them as normal equations. Begin with the theory of linear differential equations. The hypergeometric function

$$F(\alpha, \beta, \gamma, x) = 1 + \frac{\alpha \cdot \beta}{1 \cdot \gamma} x + \frac{\alpha \cdot \alpha + 1 \cdot \beta \cdot \beta + 1}{1 \cdot 2 \cdot \gamma \cdot \gamma + 1} x^2 + \cdots$$

is a solution of a very simple differential equation $G = 0$ of the second order. For variable α, β, γ, it represents a new transcendent; but for certain special values of these parameters it reduces to the elementary functions; *e. g.* it may become algebraic. In seeking for all these latter cases Schwarz was led to introduce a new variable s* which for certain values of α, β, γ satisfies the equation

$$J(s) = 1728\, x f^5(s) - H^3(s) = 0$$

where $f(s) = s(s^{10} + 11s^5 - 1)$ and $H(s) = s^{20} - 288s^{15} + 494s^{10} + 288s^5 + 1$. This equation $J = 0$ stands in so intimate relation with the icosahedron that it is called the icosahedral equation. In fact if we project stereographically the icosahedron on the s-plane, the centre being at the origin, the 12 vertices and the middle points of the 20 faces will be precisely the roots of F and H, respectively.

From this it is easy to conclude that the group of $J = 0$ is formed of the group of 60 rotations belonging to the icosahedron, §59. This group, abstractly considered, is identical with A_5. Klein has shown that the icosahedral equation whose roots are very simple known functions of $F(\alpha, \beta, \gamma, x)$ can be put in connection with $Q = 0$; it may thus be considered as a normal resolvent of $Q = 0$.

Another normal resolvent, one which springs from the elliptic functions, is the following. In trigonometry, one of the problems is to express $\sin x/n$ in terms of $\sin x$. Suppose for simplicity n is a prime; this requires the solution of an equation of degree $n - 1$. In elliptic functions the same problem comes up. Here the algebraic relation between, say $\wp(u/n, \omega_1, \omega_2)$ and $\wp(u, \omega_1, \omega_2)$ is of degree $n^2 - 1$. The solution of this equation depends upon an equation of degree $n + 1$, called an equation of transformation. For $n = 5$ such an equation is

$$\Delta^2 y^6 + 10\Delta y^3 - 12 g_2 y + 5 = 0$$

whose roots are

$$y = \left(\wp \frac{2\omega_1}{5} - \wp \frac{4\omega_1}{5}\right)^{-1} \text{and} \left(\wp \frac{2\omega_2 + 48r\omega_1}{5} - \wp \frac{4\omega_2 + 96r\omega_1}{5}\right)^{-1},$$

$$r = 0, 1, 2, 3, 4$$

Here Δ is the discriminant, $g_2^3 - 27g_3^2$.

* s is the quotient of two fundamental integrals of $G = 0$.

How equations of this type could be set in relation with the quintic was first shown by Hermite (1858).

Having found, in the elliptic functions, convenient normal resolvents for the general quintic, we might hope to employ the equations of transformation of higher orders to solve the general equations of higher degrees.

The consideration of their groups, however, shows very easily that this is not possible. To find suitable equations we must pass from the elliptic to the hyperelliptic functions. By their aid, the general equation of every degree can be solved.

BIBLIOGRAPHY.

We give here a few references for those who may wish to do collateral reading or to go deeper into the subject.

TEXT BOOKS:

H. Weber, *Algebra*, 2 vols., 2° ed.; Braunschweig 1898.
C. Jordan, *Traité des substitutions*; Paris 1870.
É. Galois, *Oeuvres Mathématiques*; Ed. by E. Picard; Paris 1897.
E. Netto, *Substitutionentheorie*, etc., Leipzig 1882. Trans. by F. N. Cole, 1892.
" " *Algebra*, 2 vols., Leipzig 1896.
L. Bianchi, *Teoria dei sostituzioni* etc., Pisa 1897 (Lithog.).
W. Burnside, *Theory of Groups*, Cambridge, Eng., 1897.

REFERENCES TO SEPARATE §§.

§2 Kronecker, *Werke*, vol. 2, pp. 248–251.
§11 Weber, *l. c.*, vol. 1, p. 41.
§12 " " " " " pp. 517–521.
§19 Bolza, *Math. Annalen*, vol. 42, p. 253.
§31 C. Jordan, *l. c.*, pp. 286–291.
Kronecker, *Berliner Berichte*, 1877, p. 846.
§38 Miller, *Bull. Amer. Math. Soc.*, Feb. 1899, p. 227.
§39 Weber, *l. c.*, pp. 49 *ff.*
§46 Kneser, *Crelle*, vol. 106, pp. 51–52.
Hölder, *Math. Annalen*, vol. 38, p. 309, 2° note.
§47 Abel, *Oeuvres*, vol. 1, p. 66.
Kronecker, *Berliner Berichte*, 1879, p. 205.
§50 M. Cantor, *Geschichte der Mathematik*, 2° ed., vol. 1, pp. 199, 219, 220.
§51 Gauss, *Disquisitiones Arithmeticæ*, Chap. 7.
Bachmann, *Kreistheilung*, Leipzig 1872.
§52 C. Jordan, *l. c.*, pp. 291–297.
Weber, *l. c.*, vol. 1, Chaps. 12, 16; vol. 2, Chaps. 22–24.
§53 Cantor, *l. c.*, *Cf.* Index, *Dreitheilung*.
§54 Hölder, *Math. Annalen*, vol. 38, p. 307.
§55 Weber, *l. c.*, pp. 652–655.
Ruffini, *Teoria generale delle equazioni* etc., Bologna 1799.
H. Burkhardt, *Zeitschrift f. Math. u. Phys.*, vol. 37, Suppl., p. 119 (1892).
Abel, *l. c.*

§59 Cayley, *Math. Papers*, vol. 2, p. 123.
C. Jordan, *Bull. Soc. Math. France*, vol. 1, p. 48.
Hölder, *Math. Annalen*, vol. 34, p. 26.
Burnside. *l. c.*

§62 F. Klein, *Das Ikosaeder*, Leipzig 1884.
Kiepert, *Crelle*, vol. 87, p. 114.
C. Jordan, *l. c.* pp. 372–382.
Lindemann, *Göttinger Nachrichten*, 1884, p. 245; 1892, p. 292.

For further references we refer to the *Encyclopädie der Mathematischen Wissenschaften*, Leipzig, Teubner: on Galois' Theory, O. Hölder, vol. 1, p. 480; on Groups, H. Burkhardt, vol. 1, p. 208; A. Wiman, vol. 1, p. 522; on Rational Functions of One or More Variables, E. Netto, vol. 1, p. 227 and p. 255; K. Vahlen, vol. 1, p. 449.

New Haven, Conn., August 1900.

CONTENTS.

PAGE

Wiener's Theory of Displacements, with an Application to the Proof of Four Theorems of Chasles. By Mr. ARTHUR SULLIVAN GALE, . 1

The Complex of Axes of a Central Quadric Surface. By Mr. EDWARD V. HUNTINGTON, ... 8

Galois' Theory of Algebraic Equations. Part II. Irrational Resolvents. By PROFESSOR JAMES PIERPONT, ... 22

ANNALS OF MATHEMATICS.

Published in October, January, April, and July, under the auspices of Harvard University, Cambridge, Mass., U. S. A.

Cambridge: Address *The Annals of Mathematics*, 2 University Hall, Cambridge, Mass., U. S. A. Subscription price, $2 a volume (four numbers) in advance. Single numbers, 75c. All drafts and money orders should be made payable to Harvard University.

London: Longmans, Green & Co., 39 Paternoster Row. Subscription price, 8 shillings a volume (four numbers) in advance.

Leipsig: Otto Harrassowitz, Querstrasse 14. Subscription price, 8 marks a volume (four numbers) in advance.

PRINTED BY THE SALEM PRESS CO., SALEM, MASS., U. S. A.